

COLEGIO DE POSTGRADUADOS

**INSTITUCIÓN DE ENSEÑANZA E INVESTIGACIÓN EN CIENCIAS
AGRÍCOLAS**

CAMPUS MONTECILLO

**POSTGRADO DE SOCIOECONOMÍA, ESTADÍSTICA E INFORMÁTICA
ECONOMÍA**

**ANÁLISIS SOBRE EL ORIGEN, COMPORTAMIENTO Y CRECIMIENTO
DEL MERCADO DEL BITCOIN**

NOMBRE DEL SUSTENTANTE
VICTOR MANUEL GONZALEZ SOLTERO

T E S I S
PRESENTADA COMO REQUISITO PARCIAL
PARA OBTENER EL GRADO DE :

MAESTRO EN CIENCIAS

MONTECILLO, TEXCOCO, EDO. DE MÉXICO.

2014

La presente tesis titulada: **Análisis sobre el origen, comportamiento y crecimiento del mercado del Bitcoin**. realizada por el alumno: **Victor Manuel González Soltero** bajo la dirección del Consejo Particular indicado, ha sido aprobada por el mismo y aceptada como requisito parcial para obtener el grado de:

MAESTRO EN CIENCIAS
SOCIOECONOMÍA ESTADÍSTICA E INFORMÁTICA
ECONOMÍA

CONSEJO PARTICULAR

CONSEJERO



Dr. David Hebert Del Valle Paniagua

ASESOR



Dr. Oscar Antonio Arana Coronado

ASESOR



Dr. Juan Ricardo Bauer Mengelberg

Montecillo, Texcoco, Estado de México, Marzo de 2014.

AGRADECIMIENTOS

Al Consejo Nacional de Ciencia y Tecnología (CONACYT), por el apoyo económico brindado para finalizar esta etapa.

Al Colegio de Postgraduados (COLPOS) y al Programa de Socioeconomía Estadística e Informática-**Economía** por brindarme el conocimiento necesario para realizar el presente trabajo.

A los integrantes de mi Consejo Particular y profesores:

Dr. David Herbert Del Valle Paniagua por darme la oportunidad de desarrollarme profesionalmente con este trabajo, por creer en mi; gracias por guiarme en todo el trayecto de este viaje, por el apoyo, conocimiento y empuje brindado.

Dr. Juan Ricardo Bauer Mengelberg por la dedicación y atención a los detalles del proyecto, por su apoyo constante, su apertura al tema, y el conocimiento compartido.

Dr. Oscar Antonio Arana Coronado por el conocimiento y el apoyo durante el proyecto.

Dr. Miguel Angel Martínez Damian por la confianza, por brindarme luz y esclarecer las dudas sobre el tema, por darme certeza y la claridad que el tema demandaba.

Dr. José Saturnino Mora Flores por ser un excelente maestro, gracias por instruirme y por complementar con bases sólidas mi formación con sus enseñanzas.

DEDICATORIA

Quiero dedicarles esta tesis a todas esas personas que estuvieron involucradas de cierta forma con el hecho de que pudiera llevarla a cabo. A mis abuelos y a mi padre, por ser un apoyo incondicional durante toda mi vida. Gracias por estar siempre cuidándome, guiándome, aconsejándome y sobre todo por su apoyo incondicional en cada proyecto que decido emprender. A mi hermano Ricardo un modelo que siempre he admirado; gracias por estar conmigo a pesar de la distancia.

A mi prima Araceli por mantenerme siempre orgulloso de ser quien soy y por apoyarme alegremente en todos mis intentos. Y en especial a mis Amigos que estuvieron al pendiente día con día al “pie del cañón” apoyándome cada uno a su forma Areli, Vianey, Luis, Gil. Azucena gracias por la confianza que con los años ha traído una amistad inquebrantable esta tesis es mía pero la maestría es nuestra.

ANÁLISIS SOBRE EL ORIGEN, COMPORTAMIENTO Y CRECIMIENTO DEL MERCADO DEL BITCOIN

Victor Manuel González Soltero

Colegio de Postgraduados, 2014

RESUMEN

Bitcoin es una moneda digital, descentralizada y parcialmente anónima. Su sistema está basado en una red punto a punto, donde no se requiere un tercero para realizar transacciones; también utiliza algoritmos criptográficos, para mantener su integridad. Esta moneda es ideal para consumidores en general y comerciantes.

Si se toma en cuenta que salió al mercado en enero de 2009 y que para octubre del 2011 superó el valor del dólar posicionándose en 2 USD por 1 Bitcoin y para el año 2013 en diciembre alcanzo los 100 USD por Bitcoins, el Bitcoin ha demostrado en su corto tiempo de vida ser una moneda útil y popular entre la gente, tanto para las personas que emprenden negocios por internet, como para organizaciones que viven de donativos. Por otro lado la mayoría de los gobiernos de todo el mundo tienen sus reservas, pues su uso se presta a fines ilícitos por su carácter anónimo.

Aunque la economía Bitcoin está floreciendo, los usuarios están preocupados por la situación legal de Bitcoin y la posibilidad de un bloqueo gubernamental. Esto podría llevar a una disminución en su consumo e incluso a una saturación del mercado de bitcoins puesto que su emisión es constante.

El siguiente tiene como objetivo demostrar mediante tasas de crecimiento el comportamiento del mercado de Bitcoins evaluando el volumen de transacciones contra el volumen de Bitcoins en circulación.

Palabras clave: Bitcoin, Criptomoneda, Moneda digital, Moneda, Criptografía.

ANALYSIS OF THE ORIGIN, BEHAVIOR AND GROWTH OF BITCOIN MARKET

Victor Manuel González Soltero

Colegio de Postgraduados, 2014

ABSTRACT

Bitcoin is a digital, decentralized and partially anonymous currency. Its system relies on a peer-to-peer networking which does not require a third party to conduct transactions; it also uses cryptography algorithms to maintain its integrity.

Taking into account it came out to market in January 2009 and by October 2011 surpassed the value of the dollar positioning itself at 2 USD for 1 Bitcoin and in December 2013 reached 100 USD per Bitcoins, the Bitcoin has shown in its short lifetime to be a useful and popular currency for people starting businesses online as well as for organizations living donations. On the other side most governments around the world hate since it lends itself to unlawful purposes due to its anonymous nature.

Although the Bitcoin economy is flourishing, users are anxious about Bitcoin's legal status and the possibility of a government crackdown. This could lead to a decrease in its consumption or even market saturation of bitcoins since its emission is constant.

The present work aims to demonstrate by using growth rates of Bitcoins market behavior evaluating the volume of transactions against the volume of Bitcoins in circulation.

Keywords: Bitcoin, Criptomoneda, Digital Currency, Currency, Cryptography.

CONTENIDO

AGRADECIMIENTOS	II
DEDICATORIA	II
RESUMEN	III
ABSTRACT	IV
CONTENIDO	V
ÍNDICE DE CUADROS	VII
ÍNDICE DE FIGURAS.....	VIII
CAPÍTULO 1: INTRODUCCIÓN	10
1.1 Estado del Tema.....	10
1.1.1 <i>Objetivos</i>	11
1.1.2 <i>Hipótesis</i>	11
1.2 El dinero y la moneda.....	11
1.3 ¿Qué es Bitcoin?	12
1.4 ¿Cómo funcionan los Bitcoins?	13
1.5 Marco Teórico.....	13
CAPÍTULO 2: ANTECEDENTES	15
2.1 Criptografía.....	15
2.1.1 <i>Algoritmos de encriptación</i>	15
2.1.2 <i>Funciones Hash</i>	16
2.1.3 <i>Firma digital</i>	16
2.2 Dinero.....	17
2.3 Moneda.....	18
2.4 Monedas electrónicas.....	18
2.5 Eventos destacados en la historia del Bitcoin.....	19
CAPÍTULO 3: MATERIALES	26
3.1 Hardware y Software	26
3.2 Bitcoin.....	30

3.2.1	<i>Bitcoin como criptomoneda</i>	31
3.3	Sistema Bitcoin.....	32
3.3.1	<i>Direcciones</i>	32
3.3.2	<i>Llaves</i>	37
3.3.3	<i>Transacciones</i>	39
3.4	Minería y mineros.....	41
3.4.1	<i>Prueba de trabajo</i>	48
3.4.2	<i>Red</i>	52
3.4.3	<i>Incentivos</i>	53
3.5	Anonimato.....	54
3.6	Seguridad.....	56
3.6.1	<i>Sistema</i>	56
3.6.2	<i>Transacciones</i>	57
3.6.3	<i>Participantes</i>	60
CAPÍTULO 4: PERCEPCIONES		63
4.1	Expertos en Tecnologías de la Información.....	63
4.2	Economistas.....	64
4.3	Gobierno.....	66
4.4	Usuario Final.....	69
CAPÍTULO 5: MÉTODOS		70
5.1	Tasas de Crecimiento.....	70
5.2	Regresión Lineal.....	73
CAPÍTULO 6: RESULTADOS Y DISCUSIÓN		75
6.1	Resultados del Análisis.....	75
CAPÍTULO 7: CONCLUSIONES		77
7.1	Bitcoin.....	77
7.1.1	<i>Ventajas</i>	77
7.1.2	<i>Desventajas</i>	78
7.2	Análisis.....	79
BIBLIOGRAFÍA		80
GLOSARIO		85

ÍNDICE DE CUADROS

CUADRO 2.1: EVENTOS HISTÓRICOS DEL BITCOIN.....	19
CUADRO 3.1: EJEMPLO DE TRANSACCIONES BITCOIN.	45
CUADRO 3.2: TRANSACCIÓN PEER TO PEER: MONTO DE BITCOINS POR DIRECCIÓN.	61
CUADRO 5.1: RESULTADOS: TASAS DE CRECIMIENTO.....	71
CUADRO 6.1: RESULTADOS ESTADÍSTICOS DE LA REGRESIÓN.....	75

ÍNDICE DE FIGURAS

FIGURA 2.1: INICIOS DEL BITCOIN, EVENTOS DEL (CUADRO 2.1) Y VALOR EN DÓLARES POR UNIDAD DE BITCOIN.	24
FIGURA 2.2: VALOR HISTÓRICO (MAYO 2013 A FEBRERO 2014) EN DÓLARES POR UNIDAD DE BITCOIN.	25
FIGURA 3.1: ACERCA DE BITCOIN MONEDERO QT. (BITCOIN.ORG 2009)	26
FIGURA 3.2: LOGO DE MACMINER.	27
FIGURA 3.3: ACERCA DE XCODE. (APPLE 2014).....	27
FIGURA 3.4:LOGO OSX MAVERICKS.	28
FIGURA 3.5: ACERCA DE MACBOOK PRO 13 PULGADAS.....	28
FIGURA 3.6: ACERCA DE MACBOOK PRO 15 PULGADAS.....	29
FIGURA 3.7: MODELO DE PRIVACIDAD.....	30
FIGURA 3.8: LOGO QUE USAN LOS COMERCIOS PARA DENOTAR QUE ACEPTAN BITCOINS.....	31
FIGURA 3.9: SOFTWARE BILLETERAS BITCOINS.	32
FIGURA 3.10: MONEDERO BITCOIN-QT: INICIO.	33
FIGURA 3.11: BILLETERA BITCOIN-QT.	34
FIGURA 3.12: MONEDERO BITCOIN-QT: ALTA DE DIRECCIÓN.....	35
FIGURA 3.13: MONEDERO BITCOIN-QT: VARIAS DIRECCIONES.....	36
FIGURA 3.14: MONEDERO BITCOIN-QT: VERIFICAR MENSAJE.	37
FIGURA 3.15: MONEDERO BITCOIN-QT: FIRMAR MENSAJE.	38
FIGURA 3.16: REPRESENTACIÓN DE UN BITCOIN MEDIANTE EL HISTORIAL DE SUS TRANSACCIONES.	39
FIGURA 3.17: MONEDERO BITCOIN-QT: TRANSACCIONES.....	40
FIGURA 3.18: SERIE DE BLOQUES BITCOIN.....	41
FIGURA 3.19: “GENESIS BLOCK” PRIMER BLOQUE DE BITCOIN.	42
FIGURA 3.20: BLOQUE: ALMACENAMIENTO DE TRANSACCIONES EN FORMA DE ÁRBOL.	43
FIGURA 3.21: MONEDERO BITCOIN: RECUPERANDO BLOQUES.....	44
FIGURA 3.22: PROCESO DE MINERÍA.....	46
FIGURA 3.23: SOFTWARE DE MINERÍA, CGMINER PARA MAC.	47

FIGURA 3.24: SOFTWARE DE MINERÍA, MACMINER.	47
FIGURA 3.25: PROOF-OF-WORK: CADENA DE BLOQUES.	48
FIGURA 3.26: BLOCK HEADER: ENVIÓ DE DATOS.	50
FIGURA 3.27: BLOCK HEADER: CONCATENACIÓN DE DATOS.....	50
FIGURA 3.28: BLOCK HEADER: CONVERSIÓN A BINARIO.....	51
FIGURA 3.29: BLOCK HEADER: PRIMER SHA256.....	51
FIGURA 3.30: BLOCK HEADER: SEGUNDO SHA256.....	51
FIGURA 3.31: BLOCK HEADER: INTERCAMBIO DE POSICIONES DEL HASH.	51
FIGURA 3.32: MÁQUINA PARA MINERÍA BUTTERFLYLABS.....	53
FIGURA 3.33: EJEMPLO DE TRANSACCIÓN GENERAL.....	54
FIGURA 3.34: DIRECCIÓN DE BITCOINS (GENERAL)	55
FIGURA 3.35: TRANSACCIÓN SIN CONFIRMAR.	57
FIGURA 3.36: TRANSACCIÓN DETALLADA.....	59
FIGURA 3.37: TRANSACCIONES PEER TO PEER.....	60
FIGURA 3.38: SISTEMA BITCOIN TRANSACCIÓN. FUENTE: (TRUEECONOMICS. 2013).....	62
FIGURA 4.1: SITIO DEEP WEB: VENTA DE IDENTIFICACIONES FALSAS.	66
FIGURA 4.2: SITIO DEEP WEB: VENTA DE DROGAS, PRESCRIPCIONES Y OTROS.	67
FIGURA 4.3: SITIO DEEP WEB: LAVADO DE BITCOINS.	68
FIGURA 5.1: VOLUMEN DE TRANSACCIONES BITCOIN.	70
FIGURA 5.2: VOLUMEN DE BITCOINS EN CIRCULACIÓN.....	71
FIGURA 5.3: COMPARACIÓN DE TASAS DE CRECIMIENTO.....	72
FIGURA 5.4: LOGARITMO DE TRANSACCIONES Y VOLUMEN EN CIRCULACIÓN DE BITCOINS.	73
FIGURA 5.5: REGRESIÓN LINEAL.	74
FIGURA 7.1: PAÍSES Y SU POSTURA SOBRE LA LEGALIDAD DEL BITCOIN.	78

CAPÍTULO 1: INTRODUCCIÓN

1.1 Estado del Tema.

Hoy en día una llamada de larga distancia es más costosa que enviar un correo electrónico: la primera presenta distintos costos según la duración y la localidad, mientras que la segunda tiene un mismo precio sin importar el destino. Esta situación se repite constantemente en otras facetas de nuestra vida cotidiana, donde los adelantos tecnológicos superan la organización y los modelos establecidos.

Algo similar está sucediendo con el auge del comercio electrónico, donde todo tipo de empresas pueden enviar y recibir productos de distintas partes del mundo.

La conversión y transferencia de divisas entre regiones es una constante, aunque los bancos actualmente tienen un modelo que atiende estos eventos, presenta ciertas desventajas cuando se compara con lo que parece ser una creativa solución tecnológica llamada **criptomoneda** (elBitcoin.org 2011).

Una de estas criptomonedas, específicamente el **Bitcoin**, está tomando fuerza en el mercado global. Hay países como India donde su demanda presenta un crecimiento considerable (The Hindu 2013).

Una pregunta que se quisiera contestar es: ¿El Bitcoin va a continuar en circulación o saldrá de uso?.

1.1.1 Objetivos.

- El objetivo del presente trabajo es conocer el comportamiento del crecimiento del mercado de Bitcoins; mediante el uso de tasas de crecimiento y una regresión lineal usando el volumen de transacciones y de Bitcoins en circulación.
- Marcar una base teórica sobre el origen, funcionamiento general y comportamiento del Bitcoin. Proporcionando un resumen del sistema sobre el que esta montado, la red y las características del Bitcoin, que sirva como base de consulta para investigaciones futuras.

1.1.2 Hipótesis.

- El mercado del Bitcoin se saturará. Debido a que hay una emisión constante de Bitcoins
- La información sobre el Bitcoin es escasa, ambigua y poco digerida para investigadores de áreas no relacionadas con la computación e informática.

1.2 El dinero y la moneda.

El dinero es cualquier medio de intercambio generalmente aceptado por una sociedad y que es usado para el pago de bienes, servicios y obligaciones. Para que un bien pueda ser calificado como dinero, debe satisfacer tres criterios principales en cuanto a su funcionalidad: Medio de intercambio, Unidad contable y Conservación de valor (Wikipedia 2012).

La moneda es una representación del dinero, aceptada por la sociedad y respaldada por un gobierno.

En el pasado la moneda y el dinero eran lo mismo; con el paso del tiempo por cuestiones de practicidad estos conceptos se separaron. Otro aspecto importante del dinero moderno es el cómo se genera. Anteriormente era respaldado por un recurso; en la actualidad esto es un supuesto pero no una realidad (elBitcoin.org 2011).

1.3 ¿Qué es Bitcoin?.

Bitcoin es una criptomoneda, virtual, descentralizada, que usa **algoritmos criptográficos**. Fue ideada en el 2008 y concebida en el año 2009, por una o varias personas bajo el seudónimo de “Satoshi Nakamoto” (DomainTools 2008).

Dentro de sus principales características encontramos que usa un código abierto (**open source**), un protocolo de transferencia **peer-to-peer** y un modelo totalmente descentralizado (Fergal Reid 2012).

Esta moneda puede ser intercambiada por los propietarios de forma casi anónima y sin la necesidad de pagar costos muy elevados a algún intermediario por realizar dicha transacción (weusecoins 2011).

Cada usuario de Bitcoin puede crear tantas **carteras digitales** como requiera, hacer las transferencias que desee y mantener cierto anonimato en el uso de ellas (weusecoins 2011).

1.4 ¿Cómo funcionan los Bitcoins?.

Cualquier persona que quiera participar en el mundo de los Bitcoins debe hacer uso de un software para crear una cartera electrónica, en la que por medio de claves públicas puede enviar o recibir Bitcoins.

Cada transferencia pasa a ser validada por los nodos de la red (**mineros**). Una vez validada la **transacción**, se convierte en parte de la **cadena de bloques** – historial de bloques -.

Los Bitcoins son creados cuando algún minero resuelve los algoritmos criptográficos que están conectados con la creación de cierto bloque.

El consumo de energía respalda la creación de los Bitcoins: a medida que los algoritmos se vuelven más complejos de resolver, aumenta el consumo necesario para obtener los Bitcoins.

1.5 Marco Teórico.

Existen muchas dudas sobre este nuevo tipo de moneda. Incluso hay especialistas que la comparan con dinero digital o con sistemas intermediarios de transferencias electrónicas, como los **Linden Dollars, Facebook Credits, Amazon Coins, World of Warcraft Gold, PayPal** y demás monedas o sistemas virtuales. No se ponen de acuerdo si el Bitcoin es una moneda, es dinero, es un bien, es todo lo anterior o sólo es como el oro mismo (Olesen 2012).

A principios del año 2010, Estados Unidos decretó el uso de recetas médicas para el consumo de ciertos medicamentos y antibióticos. Esto promovió rápidamente el

uso de Bitcoins, para comprar medicamentos vía electrónica, aumentando el valor de dicha moneda y la preocupación del gobierno por regular estas transacciones (Branstad 1993).

En varias ocasiones a lo largo de estos 4 años (2009-2013), se ha predicho varias veces “el final de la era Bitcoin”. Lo que es un hecho es que actualmente el precio de un Bitcoin sobrepasa el del dólar (2013/04/31: \$93.65). Es la moneda virtual con más aceptación en la historia, con un mercado creciente y con un futuro incierto (localbitcoins 2012, Ghassan O. Karame 2012).

Hoy en día dentro de la economía pocos hablan del tema. Uno de ellos es el **Profesor Krugman**, quien escribió un artículo donde menciona a los Bitcoins como un tipo de sistema de pago electrónico y los compara con el oro (Krugman, Golden Cyberfettters 2011).

CAPÍTULO 2: ANTECEDENTES

2.1 Criptografía.

La criptografía es la disciplina de escribir un mensaje en texto cifrado buscando la protección de la información evitando su mal uso o el acceso a ésta por parte de entes maliciosos o no autorizados (Wikipedia 2012).

Para encriptar o cifrar información se utilizan complejas fórmulas matemáticas y para poder decodificarla, se tiene que proporcionar una clave como parámetro de estas fórmulas (A. AlAhmad Mohammad 2013).

Dentro del sistema Bitcoin hay tres aspectos importantes de la criptografía:

1. **Cifrado y decodificación** – Algoritmos enfocados en convertir el texto plano en texto cifrado y viceversa, usado principalmente para asegurar su confidencialidad.
2. **Funciones Hash** – Algoritmos que crean mensajes digeridos “digests” únicos, usados principalmente para validar la integridad.
3. **Firma digital** – Algoritmos que aseguran el origen del mensaje, atendiendo el problema de la autenticación.

2.1.1 Algoritmos de encriptación.

Los algoritmos de encriptación, son una serie de ecuaciones o fórmulas matemáticas utilizadas para convertir texto común y corriente a texto cifrado basado en cierta clave (Wikipedia 2012).

A lo largo de la historia los algoritmos de encriptación se han vuelto más recurrentes. Hoy con el uso de sistemas globalizados son usados ampliamente para el resguardo de la información. Sin el uso de este tipo de técnicas el robo de información se centraría en su obtención y no presentaría mayores retos al ladrón para su aprovechamiento malicioso (elBitcoin.org 2011).

2.1.2 Funciones Hash.

En la criptografía las funciones *hash* son aquellas que reciben como entrada una cadena de texto de tamaño arbitrario y la convierten a un tamaño estándar (Black 2002).

Podemos dividir las funciones *hash* entre las que tienen como objetivo principal verificar la integridad y las orientadas principalmente a la autenticación del origen del mensaje. Dentro de estas también tenemos las que usan una clave y las que no incluyen tal parámetro (Tilborg 2005).

En general estas funciones se usan para verificar la integridad de la información, ya sea para detectar errores o intentos malintencionados (Tiwari Harshvardhan, A Secure Hash Function MD-192 With Modified Message Expansion 2010).

2.1.3 Firma digital.

La firma digital es un mecanismo criptográfico usado para asegurar que cierta entidad es la originadora de cierto mensaje, permitiendo identificar la falsificación y la manipulación de su contenido. Los usos más comunes son en documentos electrónicos, software y mensajería electrónica (Tilborg 2005).

En general los algoritmos que usan la firma digital pueden asegurar que la información no contiene errores, no ha sido modificada y que el emisor de dicha información es el propietario de la misma (Tilborg 2005).

2.2 Dinero.

El dinero es un registro o medio de intercambio aceptado como pago por bienes, servicios y deudas en un determinado ambiente económico o país.

Para que un bien sea calificado como dinero debe cumplir con tres criterios en cuanto a su funcionalidad:

- Medio de cambio.
- Unidad contable.
- Preservación de valor.

Un aspecto importante del dinero moderno es su creación. Antiguamente si uno quería crear más dinero, era necesario producir más recursos.

Al separar el concepto de dinero-moneda separamos lo intangible de lo material. Del mismo modo, con la llegada del dinero circulante el vínculo entre recursos y creación del dinero se rompió, provocando que se pudiera crear cualquier cantidad de monedas sin límites.

El valor del dinero circulante depende de las regulaciones dictadas por la ley y el gobierno.

En un sentido más amplio hay que entender el dinero como algo irreal y que va más allá de lo que conocemos como dinero legal; siendo que por definición hay muchos

bienes que pueden ser considerados como dinero desde minerales como el oro y la plata, hasta cuentas de ahorro, títulos, cheques, etc.

2.3 Moneda.

Originalmente el dinero era una representación tangible de un recurso como un metal o comida. Esto le daba al dinero su unidad de valor hoy en día a esto se le conoce como moneda.

Moneda es el término que se le da a un medio tangible generalmente aceptado para el intercambio. En la actualidad la moneda que se considera legalmente como tal, es la emitida por los bancos centrales de cada país.

2.4 Monedas electrónicas.

Las monedas electrónicas son un tipo de dinero que se percibe por medios electrónicos; en general involucra el uso de redes computacionales y el internet.

Consideramos moneda electrónica a la transferencia de fondos, depósitos, oro digital, monedas virtuales, etc.

En el mundo moderno las monedas electrónicas son de suma importancia para la economía global y fundamental para el comercio electrónico.

Quizás las formas más comunes de monedas electrónicas son las representaciones de monedas reales como el dólar y euro, almacenadas por los bancos y transferidas entre cuentas de personas o empresas. También existen “monedas privadas” - que no representan a las monedas reales - como serian el Linden Dollars, Créditos de Facebook, Oro de World of Warcraft, **Loom** y Bitcoin. (Parra 2011)

2.5 Eventos destacados en la historia del Bitcoin.

Las siguientes fechas marcan los eventos más significativos en la breve y emocionante historia de esta moneda digital.

Cuadro 2.1: Eventos históricos del Bitcoin.

Fuente: (Parra 2011), (Forbes 2012), (The Hindu 2013), (bitcoin.it 2013).

#	FECHA	\$ BTC	EVENTO
1	18-ago-08	0.00	Registro del nombre del dominio "bitcoin.org". (DomainTools 2014)
2	31-oct-08	0.00	Publicación del "paper" de Bitcoin. (Nakamoto 2008)
3	03-ene-09	0.00	Se establece el primer bloque (Genesis Block) a las 18:15:05 horas (GMT) (Bitcoin Block Explorer 2013)
4	11-ene-09	0.00	Lanzamiento de la versión 0.1 del cliente Bitcoin.
5	22-may-10	0.0041	laszlo es el primer usuario en utilizar sus Bitcoins para comprar una pizza. Paga BTC 10,000 (diez mil Bitcoins por una pizza de US\$25). (bitcointalk 2010)
6	11-jul-10	0.0080	Se publica en slashdot el lanzamiento de la versión 0.3 del cliente Bitcoin, lo cual atrae un gran flujo de nuevos usuarios.
7	12-jul-10	0.08	Se inicia un aumento brusco (x10) del valor, que en 5 días pasa de US\$0.008/BTC a US\$0.08/BTC.
8	17-jul-10	0.07	Empieza a funcionar MtGox (el primer sitio de trading).
9	06-nov-10	0.23	La economía de Bitcoin supera el millón de dólares. El precio en MtGox alcanza los US\$0.50/BTC.

10	09-feb-11	0.89	El Bitcoin alcanza la paridad con el dólar estadounidense (1 Bitcoin = 1 dólar).
11	14-feb-11	1.03	Se ofrece por primera vez un automóvil a cambio de Bitcoins.
12	16-abr-11	0.94	La revista TIME publica un artículo sobre Bitcoin.
13	10-jun-11	24.73	El tipo de cambio hace un pico, superando los US\$31, para luego caer hasta los US\$10 en un lapso de cuatro días (la mayor disminución porcentual del precio hasta la fecha).
14	13-jun-11	28.14	El usuario del foro de Bitcoin allinvain anuncia que le han robado de su computadora una billetera Bitcoin con las claves privadas para acceder a BTC 25,000 (veinticinco mil Bitcoins, entonces equivalente a US\$375,000).
15	19-jun-11	20.13	Hackean la base de datos de MtGox y logran obtener el listado de 60,000 usuarios con sus respectivas contraseñas y direcciones de e-mail. Luego se supo que el algoritmo utilizado para proteger esa información era fácilmente vulnerable. Alguien accede a una cuenta del administrador de MtGox y emite ordenes de venta por miles de Bitcoins inexistentes, forzando la caída de la cotización en MtGox desde US\$17.51 hasta US\$0.01 por Bitcoin. MtGox luego anuncia que dichas transacciones serian revertidas, y suspende las actividades durante los siguiente 7 días.
16	24-jun-11	16.68	La dificultad para generar bloques supera el millón con el bloque 133056.
17	22-jul-11	14.05	Intervex Digital lanza BitCoins Mobile, la primera

			aplicación relacionada con Bitcoin para iPad.
18	26-jul-11	14.14	Bitomat , el tercer sitio de trading de Bitcoins (en orden de volumen transado), sufre la pérdida de 17,000 Bitcoins debido a un error técnico. (En el curso del siguiente mes, MtGox adquiere Bitomat e incorpora su base de datos de usuarios; los Bitcoins pagados por MtGox en esta operación son destinados al resarcimiento de los ex – usuarios de Bitomat).
19	29-jul-11	14.14	MyBitcoin , el primer servicio de billetera online, el más grande y el más completo. Se torna inaccesible para los usuarios. Miles de personas no pueden disponer de sus Bitcoins ni saben si podrán recuperarlos. Los responsables del sitio se toman una semana para informar que la seguridad del sistema había sido vulnerada por un hacker, y luego reintegran a los usuarios sólo el 49% de sus depósitos.
20	19-ago-11	11.33	Primera Conferencia y exposición Mundial de Bitcoin, en Nueva York, EE.UU.
21	20-ago-11	11.58	Primera Conferencia y exposición Mundial de Bitcoin, en Nueva York, EE.UU.
22	21-ago-11	11.63	Primera Conferencia y exposición Mundial de Bitcoin, en Nueva York, EE.UU.
23	17-nov-11	2.88	Luego de meses de lento declive, el precio del Bitcoin toca fondo en US\$2. Se inicia una etapa de rápida recuperación, apoyada en una nueva generación de servicios que apuntan al usuario no técnico.

24	25-nov-11	2.41	Conferencia Europea de Bitcoin y Tecnología del Futuro 2011 , en Praga, República Checa. Los oradores mas destacados fueron Amir Taaki, Rick Falkvinge, Max Keiser y Stefan Thomas.
25	26-nov-11	2.44	Conferencia Europea de Bitcoin y Tecnología del Futuro 2011 , en Praga, República Checa. Los oradores más destacados fueron Amir Taaki, Rick Falkvinge, Max Keiser y Stefan Thomas.
26	07-dic-11	3.07	Internet Archive , el coloso de internet dedicado a la digitalización de todo tipo de documentos, empieza a aceptar donaciones en Bitcoins. Durante los primeros dos días recibe 480 Bitcoins.
27	27-dic-11	4.11	El sitio regional de Nueva York de Wikimedia (la fundación que incluye entre sus proyectos a Wikipedia) empieza a aceptar donaciones en Bitcoins.
28	15-ene-12	6.97	Bitcoin es el tema central en un episodio de la popular serie televisiva “The Good Wife”.
29	01-mar-12	5.04	Al menos 46,000 Bitcoins son robados de “billeteras calientes” (billeteras permanentemente activas que efectúan de manera automática gran cantidad de transacciones) en un hackeo a la compañía de servicios de hosting Linode . El sitio de trading Bitcoinica y el pool de minería Slush – <i>los emprendimientos más afectados por el siniestro</i> – anuncian que continuarán funcionando con normalidad. El precio del Bitcoin se mantiene sin cambios significativos (en torno a los US\$5).

30	02-abr-12	4.89	Se anuncia en el foro de Bitcoin el lanzamiento de CoinDL , el iTunes del mundo Bitcoin.
31	30-jun-12	6.58	Ycombinator , la mayor incubadora tecnológica del mundo, anuncia que esta financiando Coinbase , un servicio de cartera Bitcoin online.
32	23-jul-12	9.33	WIKISPEED se convierte en el primer fabricante de automóviles en aceptar Bitcoins.
33	05-dic-13	1129.00	El interés del Bitcoin en India aumenta drásticamente, https://buysellbitco.in reporta un aumento en las transacciones de Bitcoins en rupias.
34	18-feb-14	558.00	Primeros cajeros automáticos Bitcoin llegan a Estados Unidos

El Bitcoin a lo largo de su trayectoria ha sufrido altibajos relacionados con sucesos dentro de su mercado, en la (Figura 2.1 y Figura 2.2), se puede apreciar la volatilidad de esta herramienta.

En menos de un año esta moneda pasó de valer poco más de 20 a 1100 dólares por Bitcoin, lo que representa un incremento del 5500% (Figura 2.2). Sin embargo también ha presentado momentos en los que su valor cae drásticamente como marca el (Cuadro 2.1) en su punto 23, donde el valor del Bitcoin bajo de 11.63 a 2.88 en menos de tres meses.

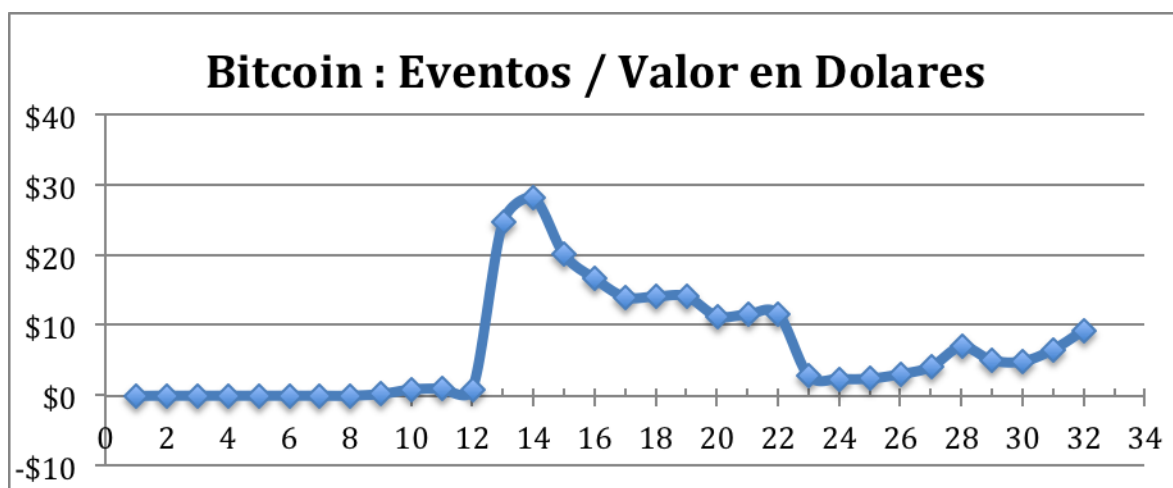


Figura 2.1: Inicios del Bitcoin, eventos del (Cuadro 2.1) y valor en dólares por unidad de bitcoin.

Fuente: (Blockchain 2013).



Figura 2.2: Valor histórico (Mayo 2013 a Febrero 2014) en dólares por unidad de Bitcoin.

Fuente: (Charts 2010).

CAPÍTULO 3: MATERIALES

3.1 Hardware y Software

Para este estudio se utilizaron como herramientas las siguientes tecnologías:

1.) **Monedero bitcoin QT versión 0.7.2-beta**: Software experimental distribuido bajo licencia Open Source que funge como cartera virtual para almacenar y realizar transferencias de Bitcoins.

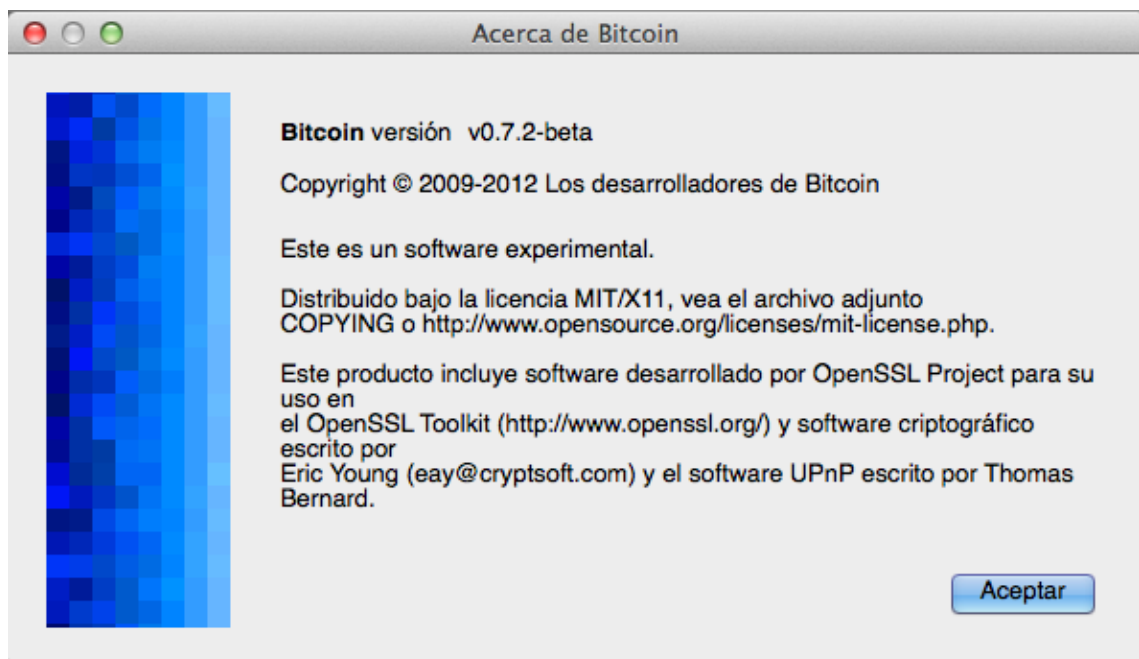


Figura 3.1: Acerca de Bitcoin Monedero QT. (bitcoin.org 2009)

2.) **CGMiner versión 4 para Mac OS 10.6+**: Software para minería multi-hilo con soporte para “*pools*” – Sitios donde se juntan usuarios para la minería en grupos - disponible bajo licencia de tipo GNU (Kolivas 2011)

3.) **MacMiner, versión 1.5.18e:** Software para minería de Bitcoins, desarrollado específicamente para la plataforma de MAC. (O'Mara 2013)



Figura 3.2: Logo de MacMiner.

4.) **Xcode versión 5.1.1:** Software IDE para desarrolladores de sistemas OS X y IOS.



Figura 3.3: Acerca de Xcode. (Apple 2014)

5.) **Sistema Operativo OSX Mavericks.** (Apple 2014)



Figura 3.4: Logo OS X Mavericks.

Todo el software antes mencionado se monto sobre plataformas Macbook Pro con las siguientes especificaciones:



Figura 3.5: Acerca de MacBook Pro 13 pulgadas.

6.) **MacBook Pro con pantalla de 13 pulgadas**, manufacturada a mediados del año 2010 con un sistema operativo OS X. Nombre código Mavericks, Versión 10.9.2

Procesador 2.4 GHz Intel Core 2 Duo

Memoria 8 GB 1067 MHz DDR3

Graficos NVIDIA GeForce 320M 256 MB

Software OS X 10.9.2 (13C64)

Dado que la minería exige un equipo con mayor potencia, para demostrar su alcance, se utilizó de forma conjunta el software de minería dentro del siguiente sistema con mayor potencia:



Figura 3.6: Acerca de MacBook Pro 15 pulgadas.

7.) **MacBook Pro con pantalla de 15 pulgadas**, manufacturada a finales del año 2011 con sistema operativo OS X. Nombre código Mavericks, Versión 10.9.2

Procesador 2.2 GHz Intel Core i7

Memoria 16 GB 1333 MHz DDR3

Graficos Intel HD Graphics 3000 512 MB

3.2 Bitcoin

Bitcoin es el nombre de un proyecto iniciado por “**Satoshi Nakamoto**”, para crear la primera criptomoneda descentralizada del mundo (Andersen 2010).

Se menciona que es descentralizada debido a su modelo de privacidad donde no se depende de una tercera entidad para realizar ninguna transacción.

Más que una criptomoneda, es un sistema de pagos basado en éxitos criptográficos, libre, descentralizado y anónimo que permite a dos entidades realizar transacciones de forma directa sin necesidad de que una tercera parte intervenga (Figura 3.1) (Nakamoto 2008).

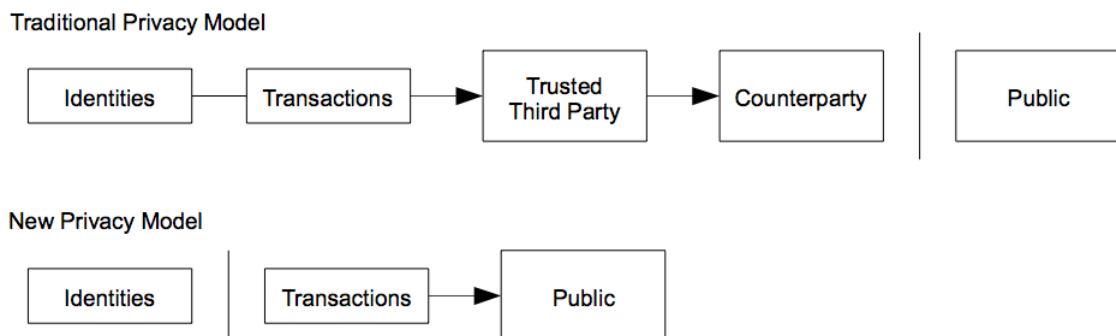


Figura 3.7: Modelo de Privacidad.

Fuente: (Nakamoto 2008).

3.2.1 Bitcoin como criptomoneda

Bitcoin es una de las primeras implementaciones de criptomoneda y ha sido la más exitosa hasta la fecha. Gran parte de su éxito se debe al enorme ecosistema que creció alrededor de esta moneda; a diferencia de sus competidoras, Bitcoin tiene mayor aceptación en el mercado, circunstancia que se puede comprobar con el aumento del precio de Bitcoins: cada vez la gente está dispuesta a pagar más por un Bitcoin.



Figura 3.8: Logo que usan los comercios para denotar que aceptan bitcoins.

Fuente: (bitcoin.it 2013).

Bitcoin es un concepto revolucionario, un proyecto que ha creado un tipo de moneda que no depende de ninguna autoridad ni de algún sistema centralizado para su control.

El valor del Bitcoin depende solamente de su inventario limitado, la ley de oferta-demanda y el costo Hash/kW para la resolución de transacciones (**minería**) (Nakamoto 2008). Su seguridad no está sujeta a ningún lugar de almacenamiento o la ubicación de su base de datos; más bien, responde a algoritmos criptográficos avanzados.

Algunas de las ventajas que tiene esta criptomoneda son su alta liquidez, bajos costos de transacción y su carácter de moneda globalizada. Por ejemplo permite que instituciones en conflicto con ciertos gobiernos puedan recibir donaciones. (Parra 2011)

3.3 Sistema Bitcoin

A continuación se da una breve explicación del Sistema Bitcoins; para información más detallada se puede acudir al texto “paper Bitcoin” (Nakamoto 2008).

3.3.1 Direcciones

Se puede considerar que las direcciones de bitcoins son como cuentas bancarias, con la diferencia de que se pueden crear tantas direcciones como el usuario quiera, incluso alentando a que se cree una por cada transacción.

El usuario comienza descargando una aplicación cliente en su computadora para crear billeteras en las cuales depositará sus Bitcoins.

Be part of the Bitcoin network

Do you have a computer that you keep switched on all the time, that's connected to the Internet? You can help the community by simply running the **full Bitcoin client** on it. The full client is more resource intensive and will take a complete day to synchronize. After that your computer will contribute to the network by checking and relaying transactions.

Desktop wallets

Desktop wallets are installed on your computer. They give you complete control over your wallet. You are responsible for protecting your money and doing backups.

Mobile wallets

Mobile wallets allow you to bring Bitcoin with you in your pocket. You can exchange bitcoins easily and pay in physical stores by scanning a QR code or using NFC "tap to pay".

Web wallets

Web wallets allow you to use Bitcoin on any browser or mobile and often offer additional services. However, you must choose your web wallet with care as they host your bitcoins.

Bitcoin-Qt **MultiBit** **Hive** **Bitcoin Wallet** **Armory** **Electrum**

Figura 3.9: Software Billeteras Bitcoins.

Fuente: (bitcoin.org 2009).

En este trabajo se usó (como referencia) el software inicial de monedero Bitcoin **Bitcoin-Qt**, ya que fue el primer cliente ofrecido por bitcoin.org. Es bastante robusto por lo tanto uno de los más seguros, aunque su uso requiere bastante paciencia (Figura 3.4).

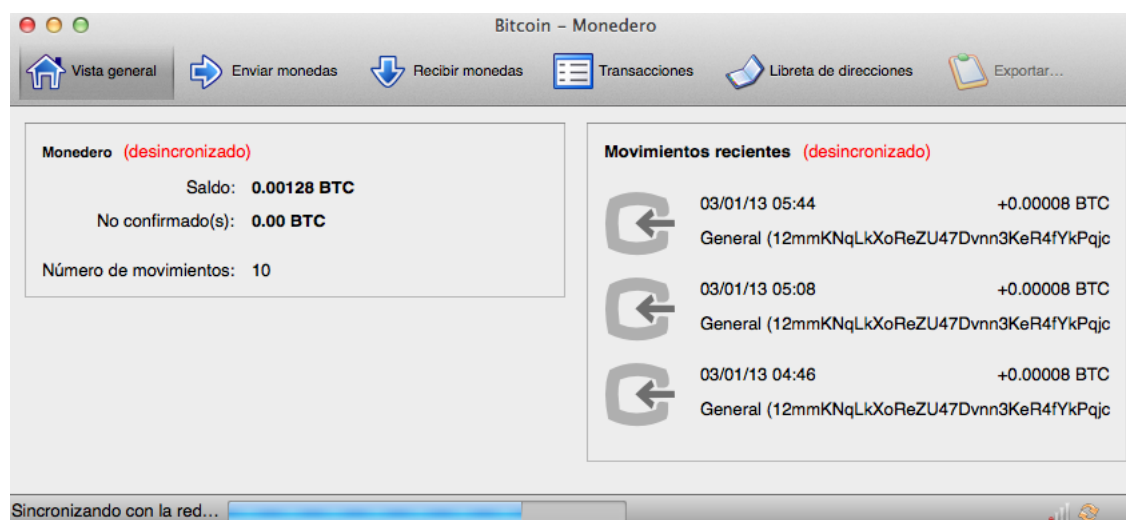


Figura 3.10: Monedero Bitcoin-Qt: Inicio.

Fuente: (elBitcoin.org 2011).

En la (Figura 3.4) se muestra una cartera funcional en el cliente Bitcoin-Qt. Se puede apreciar que su saldo es de 0.00128 BTC, el número de transacciones 10, el estado de la billetera con respecto al sistema “desincronizado” - termino que hace referencia al estado de la billetera y su relacion con el historial del sistema - y un breve resumen de las últimas transacciones verificadas (movimientos recientes).

Una billetera es un archivo que contiene una o más direcciones. Dichas direcciones son un conjunto de caracteres y números como:

“1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa”



Figura 3.11: Billetera Bitcoin-Qt.

Fuente: (elBitcoin.org 2011).

Cada software usado para crear las billeteras es desarrollado por los usuarios que participan en el sistema Bitcoin, pero sin importar el grado de complejidad o evolución del programa creado, todos tienen que sujetarse a las reglas del sistema para poder participar en él (Figura 3.5).

Una vez instalado el software cliente, el usuario creará sus direcciones para empezar a recibir y enviar bitcoins (Figura 3.6).

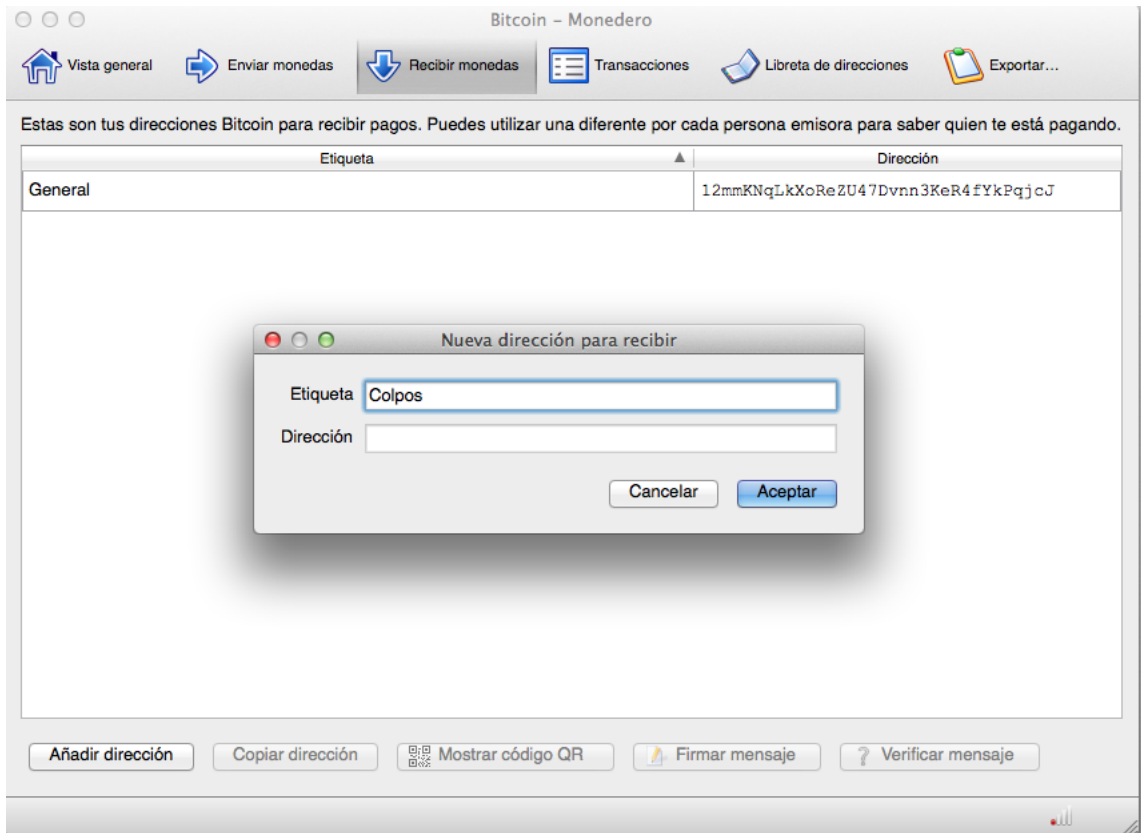


Figura 3.12: Monedero Bitcoin-Qt: Alta de dirección.

Fuente: (elBitcoin.org 2011).

En la (Figura 3.6) se muestra como el usuario da de alta una nueva dirección personal por medio del monedero. En este ejemplo se asigna una etiqueta con el valor "Colpos"; acto seguido el software genera una dirección alfanumérica.

Dicha dirección almacena una cantidad de Bitcoins. Se pueden crear tantas direcciones como se requiera, incluso se recomienda usar una dirección para cada transacción, como muestra la (Figura 3.7) donde un mismo usuario tiene dos direcciones diferentes.

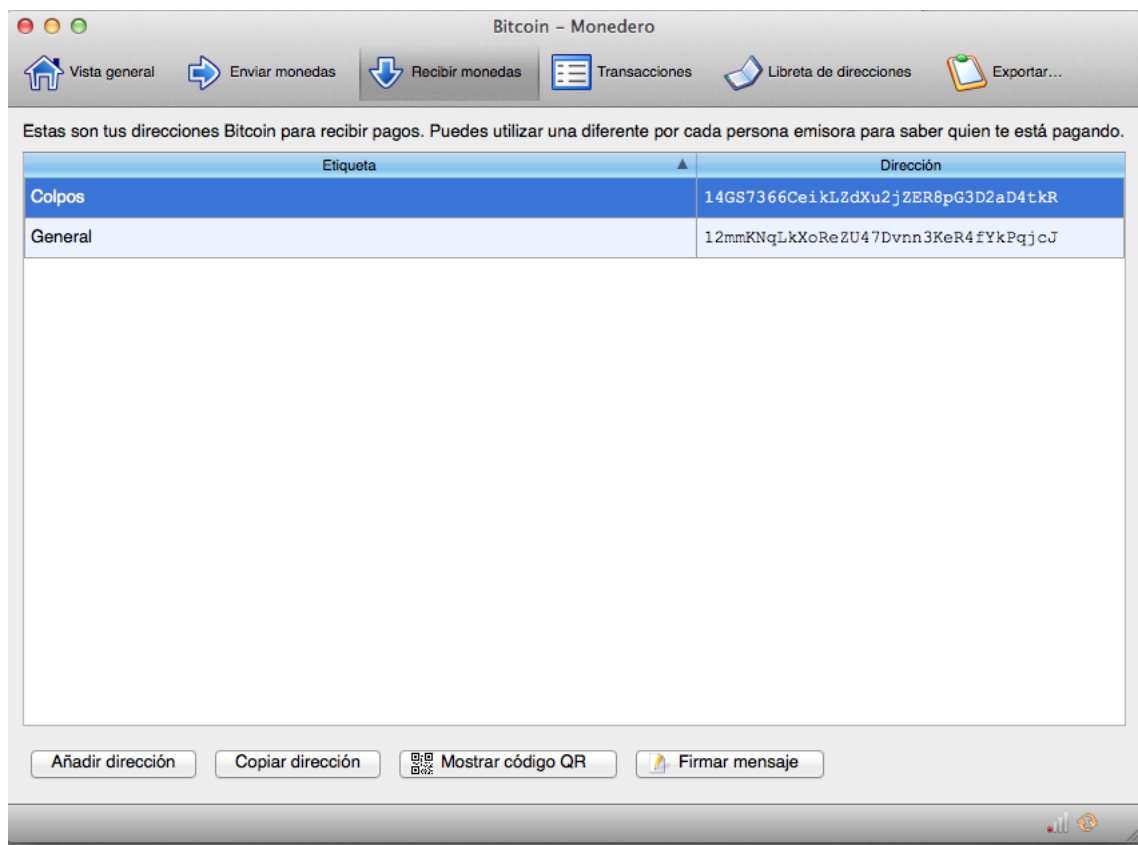


Figura 3.13: Monedero Bitcoin-Qt: Varias direcciones.

Fuente: (elBitcoin.org 2011).

3.3.2 Llaves

Las llaves - también llamadas claves - se usan dentro de un método criptográfico asimétrico. Este método se usa para el envío de mensajes donde el emisor del mensaje genera dos claves: pública y privada. La clave privada se usa para firmar el mensaje y la publica para abrirlo.

Las claves empleadas sirven para el resguardo de los Bitcoins y para validar la propiedad de los mismos (Figura 3.8).

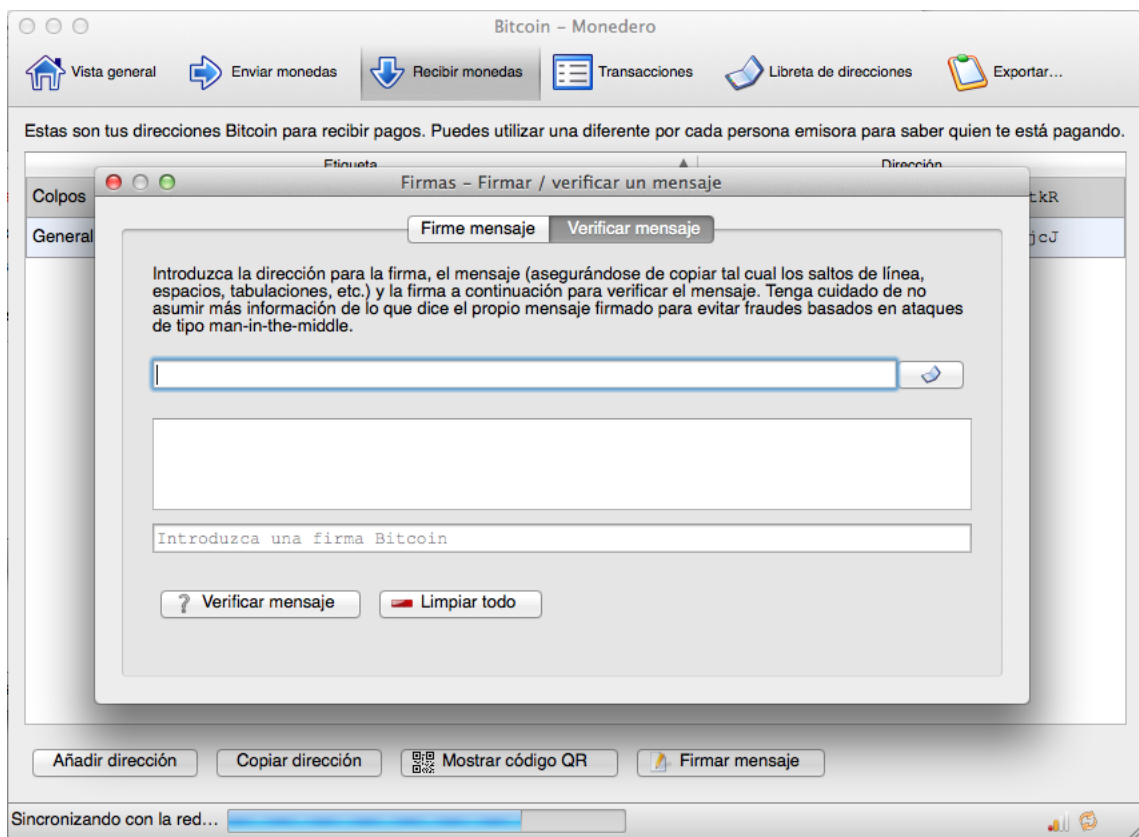


Figura 3.14: Monedero Bitcoin-Qt: Verificar mensaje.

Fuente: (elBitcoin.org 2011).

La dirección dentro de la cartera representa una clave pública conocida por todos para recibir Bitcoins, mientras que la clave privada la conoce sólo el propietario y sirve para validar la autoridad sobre la cartera (Figura 3.9).

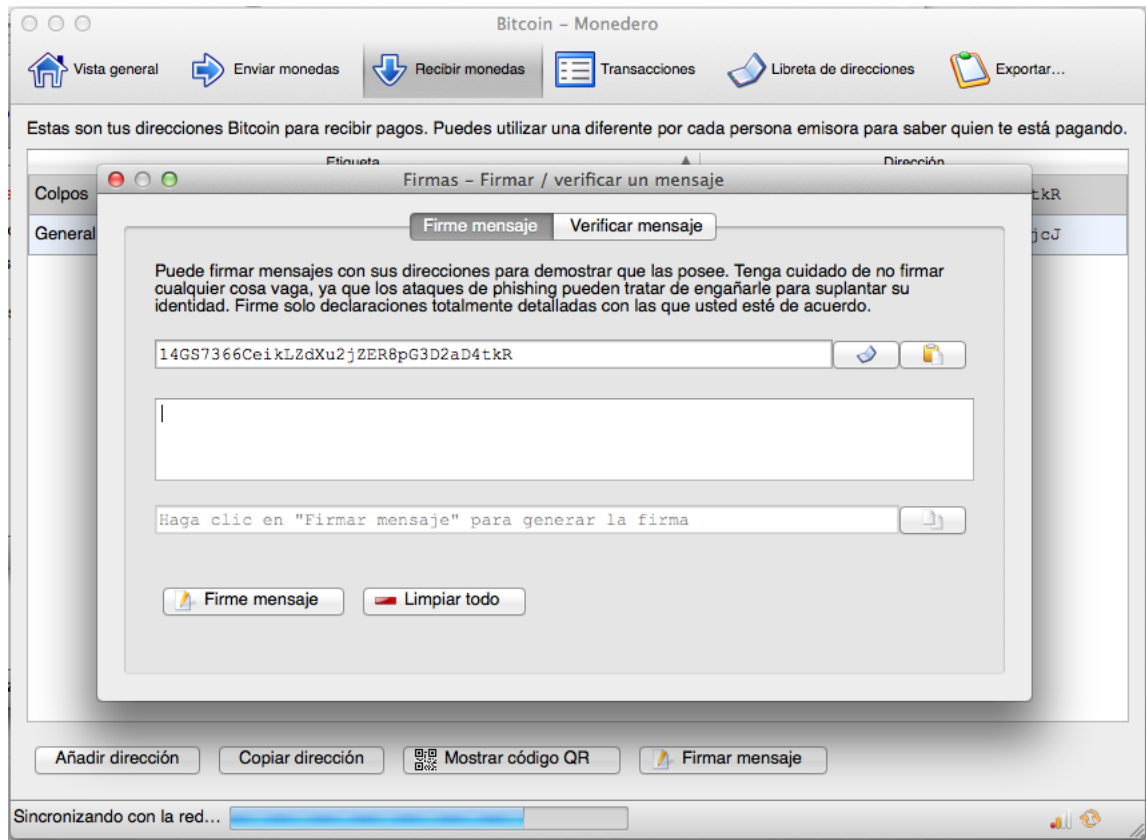


Figura 3.15: Monedero Bitcoin-Qt: Firmar mensaje.

Fuente: (elBitcoin.org 2011).

La clave pública les a que permite a las demás personas identificar que el mensaje firmado por la clave privada sea válido.

3.3.3 Transacciones

Son todos los eventos de creación, envío y recepción de Bitcoins llevados a cabo entre los distintos participantes del sistema y registradas por todos los nodos involucrados.

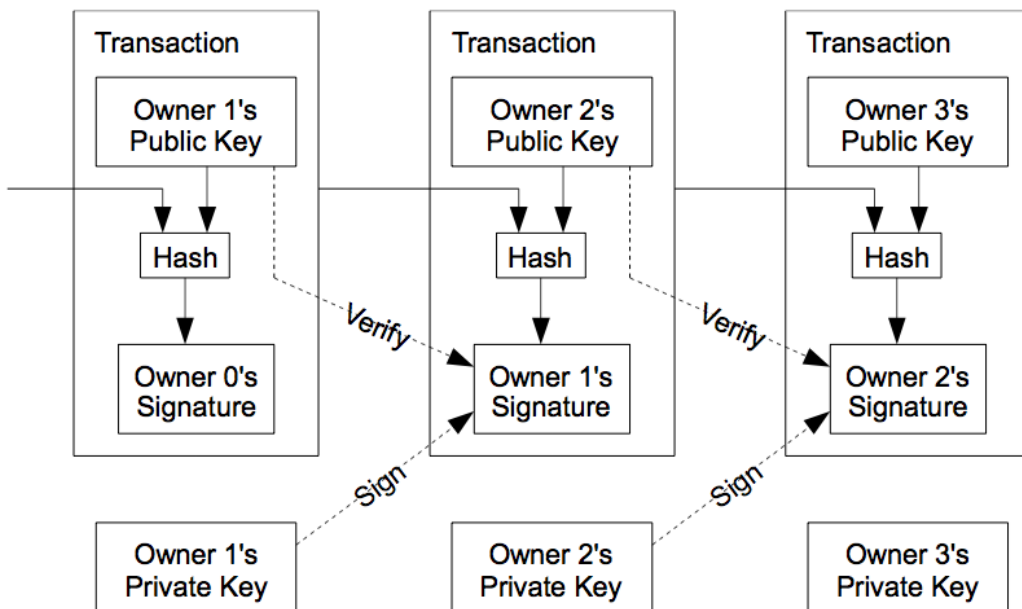


Figura 3.16: Representación de un Bitcoin mediante el historial de sus transacciones.

Fuente: (Nakamoto 2008).

En la (Figura 3.10) se muestra la cadena de transacciones que se almacenan en la moneda electrónica usando las llaves y códigos hash para ser consultados como un historial de pertenencia que autentica la posesión de la moneda. (Nakamoto 2008)

Debido a que el sistema no deposita su confianza en una tercera entidad validadora como un banco en el método actual, en su intento por tratar de prevenir el “doble gasto” considera que para tomar como válida una transacción, tiene que revisar todas las transacciones anteriores hasta la creación misma de los bitcoins que estén involucrados. Esto hace a las transacciones prácticamente irreversibles, previniendo el fraude y la duplicidad en el gasto de un mismo Bitcoin (Saito 2013).

Un usuario común puede visualizar, luego de descargar los bloques que contengan sus transacciones, el historial de sus transacciones en su monedero usando el software adecuado (Figura 3.11).

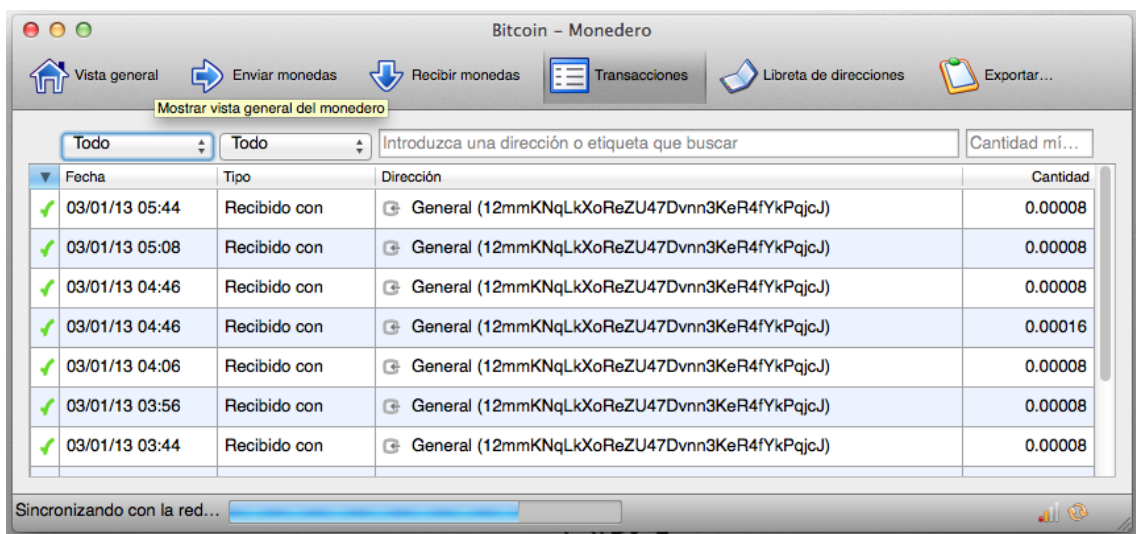


Figura 3.17: Monedero Bitcoin-Qt: Transacciones.

Fuente: (elBitcoin.org 2011) .

3.4 Minería y mineros

Para empezar a hablar de minería tenemos que entender el concepto de **bloque** y su importancia dentro del sistema Bitcoin.

Se entiende por **bloque** un conjunto de transacciones que el sistema engloba en una clave única, para controlar el espacio en memoria del historial de las transacciones (Figura 3.12). Dichos bloques son generados por el sistema cada cierto tiempo, que varía y es determinado por una ecuación que utiliza como variables el volumen de Bitcoins en circulación y el tiempo empleado en la resolución de los bloques.

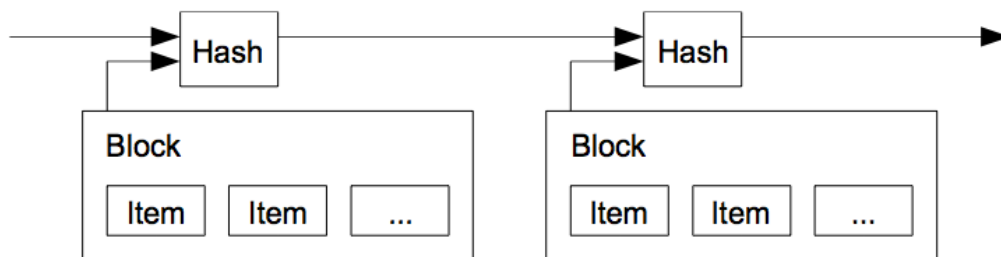


Figura 3.18: Serie de bloques Bitcoin.

Fuente: (Nakamoto 2008).

Al primero de todos los bloques dentro del sistema Bitcoin se le conoce como “Genesis Block” y fue creado el 3/01/2009. Dicho bloque contenía 50 Bitcoins que fueron enviados mediante la transacción “4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b” a la

dirección "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa" como se muestra en la (Figura 3.13).

Block 0²

Short link: <http://blockexplorer.com/b/0>

Hash²: 00000000019d6689c085ae165831e934ff763ac46a2a6c172b3f1b60a8ce26f

Next block²: [00000000839a8c6886ab5951d76f411475428afc90947ee320161bbf18eb6048](#)

Time²: 2009-01-03 18:15:05

Difficulty²: 1 ("Bits"²: 1d00ffff)

Transactions²: 1

Total BTC²: 50

Size²: 285 bytes

Merkle root²: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdada33b

Nonce²: 2083236893

[Raw block²](#)

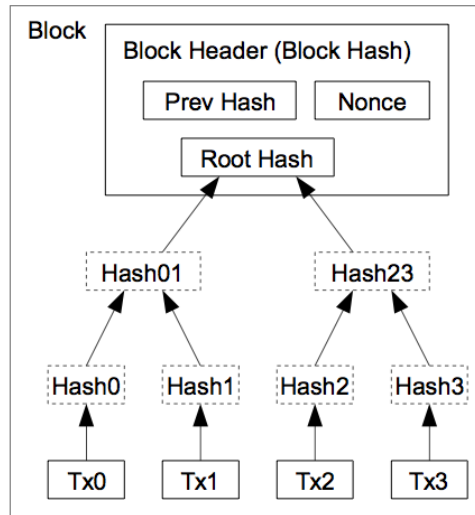
Transactions

Transaction ²	Fee ²	Size (kB) ²	From (amount) ²	To (amount) ²
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa : 50

Figura 3.19: "Genesis Block" Primer bloque de Bitcoin.

Fuente: (Bitcoin Block Explorer 2013).

Las transacciones son almacenadas por medio de sus claves en forma de árbol, lo que evita el tener que almacenar su contenido dentro de los bloques y disminuye drásticamente el tamaño final de los mismos (Figura 3.14).



Transactions Hashed in a Merkle Tree

Figura 3.20: Bloque: Almacenamiento de transacciones en forma de árbol.

Fuente: (Nakamoto 2008).

El tamaño del historial y por consiguiente la forma en la que se almacenan las transacciones es de suma importancia. Tanto para el minero como para un usuario común es necesario trabajar con el historial de las transacciones realizadas a lo largo de la historia del Bitcoin, es decir, tiene que tener todo el historial pasado de los bloques o al menos hasta donde se encuentren sus transacciones, para poder tener actualizado su saldo de Bitcoins.

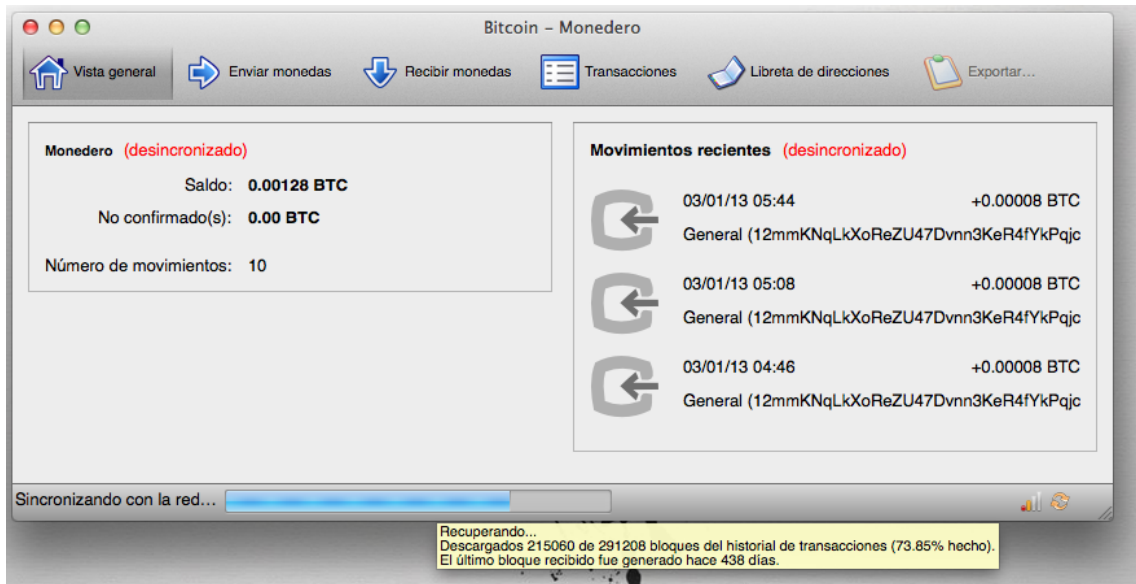


Figura 3.21: Monedero Bitcoin: Recuperando Bloques.

Fuente: (elBitcoin.org 2011)

En la (Figura 3.15) se muestra en la parte inferior una barra azul que indica el porcentaje de bloques revisados, los días transcurridos desde el último bloque recibido y también nos proporciona el numero de bloque descargado y el total de bloques existentes hasta la fecha.

Suponiendo que se genere un bloque cada 10 minutos y que el bloque sin contener ninguna transacción pesa 80 bytes; se puede deducir que en promedio estamos hablando de 4.2MB por año, de consumo en memoria (Cuadro 3.1) (elBitcoin.org 2011).

Cuadro 3.1: Ejemplo de transacciones Bitcoin.

Fuente: (Bitcoin Block Explorer 2013).

N	Hash	Tiempo	Tran	Total BTC	Tamaño (kB)
267958	468c731dea...	2013-11-04 20:06:01	307	1618.70842049	149.104
267957	975eb8df02...	2013-11-04 20:04:35	94	1648.08425906	41.659
267956	285b75885f...	2013-11-04 20:03:41	401	11267.5329959 5	194.645
267955	99abc3a1ad...	2013-11-04 19:53:53	65	680.14723688	41.241
267954	3e200bd062...	2013-11-04 19:52:41	158	3449.11340924	91.083
267953	56b5b3072f...	2013-11-04 19:51:09	157	2549.83044786	70.929
267952	60b1e7a57f...	2013-11-04 19:48:28	575	65210.4432671 1	369.901
267951	26131fe251...	2013-11-04 19:38:58	549	34836.1724112 1	249.067
267950	379e2a349c...	2013-11-04 19:21:03	370	13201.9463193	156.033
267949	94ca7e81e2...	2013-11-04 19:11:55	554	11767.0165468 7	470.798
267948	5f3913d0a5...	2013-11-04 19:00:21	571	13307.1630663 5	249.076
267947	10747d0b1f...	2013-11-04 18:45:11	651	11598.2922109 1	249.016
267946	86d6d5b17d...	2013-11-04 18:24:36	614	10907.5426675 3	248.658
267945	41b6435c26...	2013-11-04	536	20753.5061497	285.646

		18:05:07		8	
267944	7a206908f4...	2013-11-04 17:51:28	377	4468.32086374	191.846
267943	2c43b3c05c...	2013-11-04 17:40:27	73	1952.01251009	49.704
267942	7971ebe920...	2013-11-04 17:39:40	1	25	0.241
267941	949a5f0ea2...	2013-11-04 17:39:02	440	9025.72572891	219.513
267940	9e01ec9f21...	2013-11-04 17:27:00	225	4854.45890997	108.49
267939	fd097e22e4...	2013-11-04 17:22:16	534	9847.08003786	369.363

Los **mineros** son entes que aportan su poder computacional (*CPU power*), para resolver y validar un bloque mediante algoritmos criptográficos. A este proceso se le conoce como **minería** (Figura 3.16). Entre más mineros resuelvan y validen un bloque, más confiable lo vuelven, hasta el punto de considerarlo válido por toda la red (Nakamoto 2008).

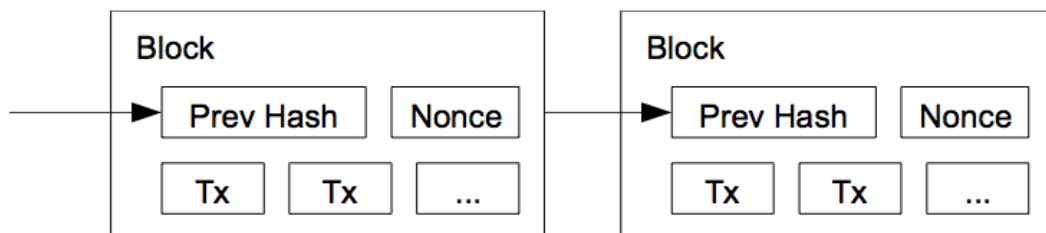


Figura 3.22: Proceso de Minería.

Fuente: (Nakamoto 2008).

La minería está abierta a todo tipo de usuarios; en sus inicios el software necesario para este propósito era demasiado técnico (Figura 3.17), lo que causó que solo participaran usuarios ávidos en el tema. Hoy en día el software para este propósito es cada vez más amigable y aún usuarios con pocos conocimientos, siguiendo guías en internet, pueden comenzar a minar (Figura 3.18).

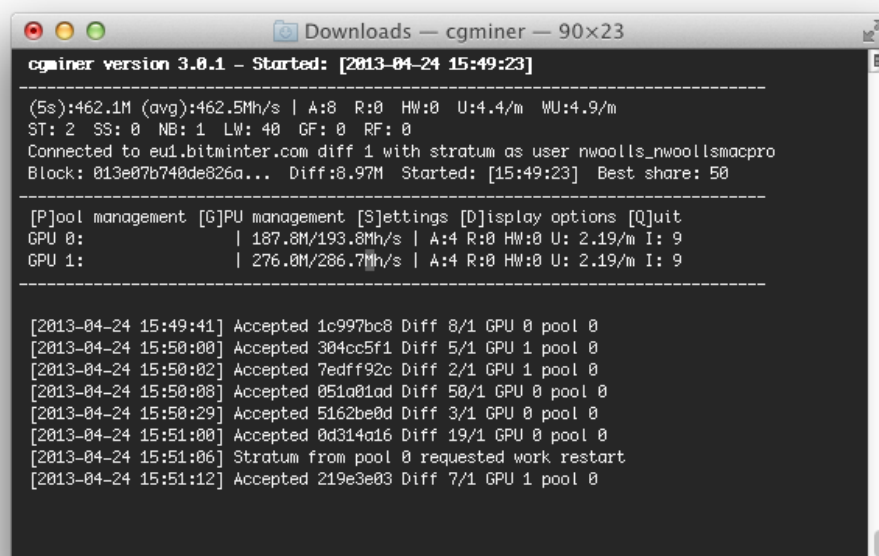


Figura 3.23: Software de Minería, CGMiner para MAC.

Fuente: (Kolivas 2011).

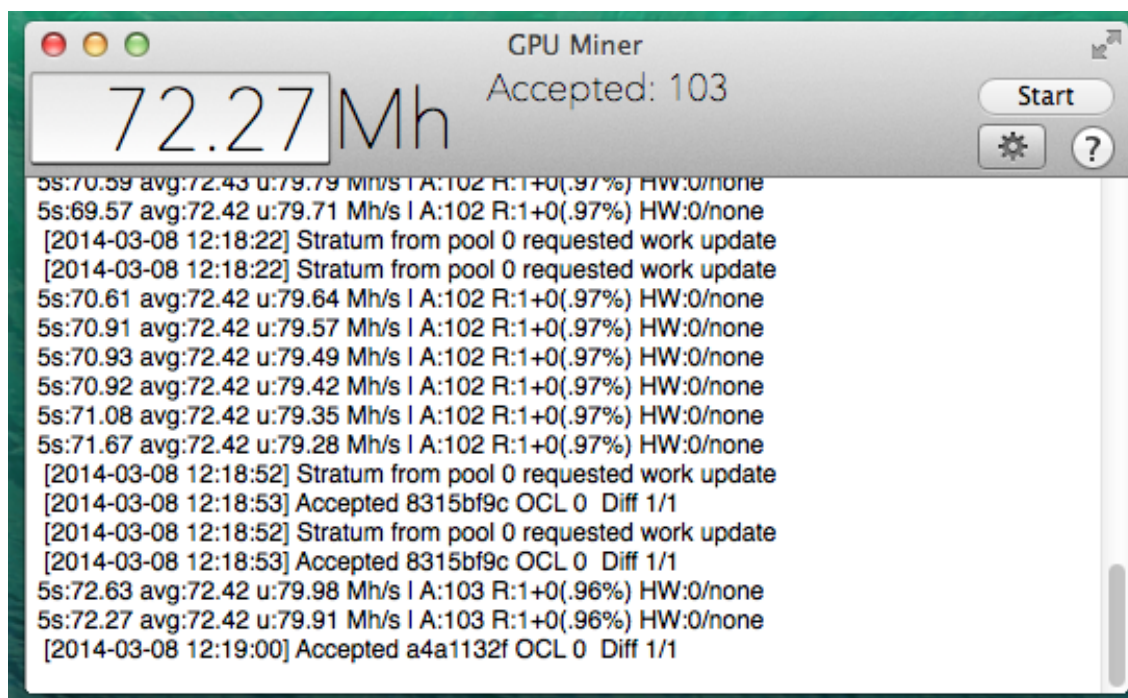


Figura 3.24: Software de Minería, MacMiner.

Fuente: (O'Mara 2013).

A nivel hardware la situación es muy similar pero en sentido inverso. En sus inicios el equipo computacional necesario para minar era relativamente sencillo: casi cualquier computadora podía con la carga de trabajo. Actualmente la cosa es distinta, puesto que debido a la complejidad de los bloques a resolver, se necesitan equipos cada vez más especializados para poder realizar la minería de Bitcoins.

3.4.1 Prueba de trabajo.

La prueba del trabajo (**poof-of-work**) se refiere al costo en tiempo y poder de procesamiento requerido para resolver un bloque.

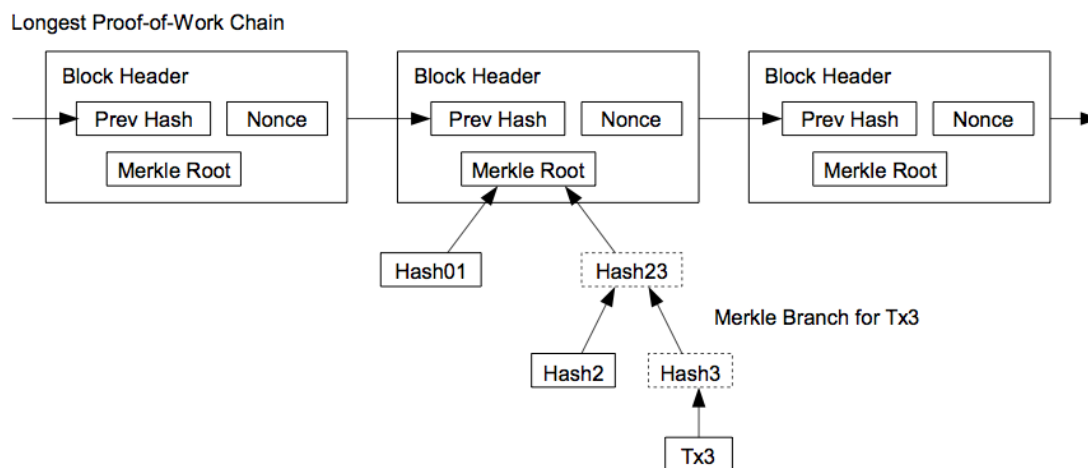


Figura 3.25: Proof-of-work: Cadena de bloques.

Fuente: (Nakamoto 2008).

En el sistema Bitcoins, resolver o validar una transacción es cuando un minero trata de encontrar una llave hash aleatoria que le genere - en combinación con el hash de la transacción anterior a la que busca atender - un formato específico con cierto número de ceros al principio, los cuales fueron insertados de manera aleatoria por

el sistema Bitcoin al momento de realizar la transacción (Figura 3.19) (Nakamoto 2008).

Conforme aumenta el volumen de transacciones y su validación, la complejidad para resolverlas crece proporcionalmente.

Una vez entendido los términos minería, minero, bloque, cadena de bloques y prueba de trabajo podemos ahondar mas en la estructura y generación de los bloques.

El proceso de la minera inicia con un algoritmo de generación de bloques que recibe como valores iniciales varios componentes que forman la cabecera (**header**) del bloque como son:

- **Versión:** Numero de versión del bloque.
- **Hash del Bloque Previo:** Hash de 256 bits que representa el header del bloque anterior.
- **Hash raíz del árbol Merkle:** Hash de 256 bits generado a partir de todas las transacciones incluidas en el bloque.
- **Hora:** Impresión de tiempo (**timestamp**) en segundos transcurridos desde la fecha 1970-01-01T00:00 UTC.
- **Bits:** Valor objetivo (**target**), el valor máximo que se debe encontrar para resolver el bloque en curso.
- **Nonce:** Numero aleatorio de 32 bits generado por el minero que inicia desde 0 y puede alcanzar 4,294,967,296 (2^{32}).

En el siguiente ejemplo, usando el código básico se muestran el proceso y los valores que un minero necesita, para generar el bloque 0 – el primer bloque del sistema –.

```

$version = littleEndian(1);
$prevBlockHash = SwapOrder('0000000000000000000000000000000000000000000000000000000000000000');
$rootHash = SwapOrder('4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b');
$time = littleEndian(1231006505);
$bits = littleEndian(486604799);
$nonce = littleEndian(2083236893);

```

Figura 3.26: Block Header: Envío de datos.

Fuente: (bitcoin.it 2013)

En la (Figura 3.20) se declaran las variables para cada una de las partes que conforman el “Block header” del bloque 0:

\$version = 1 .

\$prevBlockHash = 0 .

El bloque que lo antecede es ninguno por eso su valor es 0.

\$rootHash = 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b .

La raíz del árbol merkle de todas las transacciones contenidas en este bloque son solo una por consiguiente la raíz tiene el mismo valor que el hash de dicha transacción.

\$time = 1231006505.

Fecha y hora en que se creo el bloque en segundos en este caso 3/enero/2009, 18:15:05 GMT.

\$bits = 486604799.

\$nonce = 2083236893.

```

$header_hex = $version . $prevBlockHash . $rootHash . $time . $bits . $nonce;

```

Figura 3.27: Block Header: Concatenación de datos.

Fuente: (bitcoin.it 2013)

Una vez obtenidos los valores en su formato correspondiente, se agrupan en una sola variable formando el “block header” con el que se va a probar. (Figura 3.21)

```
$header_bin = hex2bin($header_hex);
```

Figura 3.28: Block Header: Conversión a binario.

Fuente: (bitcoin.it 2013)

El “block header” tiene que ser convertido a un formato binario antes de ser transformado a un valor sha256 (Figura 3.22).

```
$pass1 = hex2bin( hash('sha256', $header_bin ) );
```

Figura 3.29: Block Header: Primer sha256.

Fuente: (bitcoin.it 2013)

Se transforma el “block header” una primera vez a un formato sha256 y se vuelve a convertir a un formato binario (Figura 3.23).

```
$pass2 = hash('sha256', $pass1);
```

Figura 3.30: Block Header: Segundo sha256.

Fuente: (bitcoin.it 2013)

Se transforma por segunda vez el “block header” en un formato sha256 (Figura 3.24).

```
$FinalHash = SwapOrder($pass2);
```

Figura 3.31: Block Header: Intercambio de posiciones del hash.

Fuente: (bitcoin.it 2013)

Se intercambian los valores de posición y esto da por terminado el proceso de transformación, una vez obtenido este valor **\$FinalHash** se compara con el valor **target** y si es menor se ha resuelto el bloque.

3.4.2 Red.

En cuanto se refiere en cuanto a la red, el comportamiento del sistema es el siguiente:

1. Cualquier nueva transacción es enviada a todos los nodos conectados a la red.
2. Los mineros agrupan las transacciones en bloques.
3. Cada uno de los mineros busca resolver el bloque (proof-of-work).
4. Cuando un nodo encuentra una prueba de trabajo suficiente, envía el bloque a todos los nodos.
5. Los nuevos bitcoins que el sistema otorga de premio por resolver dicho bloque se envían a la cuenta del minero que resolvió primero el bloque.
6. Los nodos aceptarán el bloque como válido sólo si todas las transacciones contenidas en él son válidas.
7. Los nodos demuestran su aceptación trabajando en crear el siguiente bloque de la cadena usando la llave hash aceptada del bloque anterior.

Los nodos consideran válida a la cadena más larga de bloques y continuarán trabajando para extenderla (elBitcoin.org 2011).

3.4.3 Incentivos.

El sistema crea Bitcoins cada cierto tiempo, mismos que serán otorgados como premios a los que resuelvan el bloque del momento. Este método de incentivos hace que los nodos tengan interés en participar dentro de la red y así mantenerla. Debido a que no hay ninguna entidad central que controle, tampoco existe una entidad que administre el sistema y son los mismos participantes quienes lo mantienen. También se pueden ofrecer Bitcoins a cambio de atender una transacción, lo que mantiene interesados a los participantes en contribuir con la circulación de los Bitcoins (bitcoin.it 2013).

Es tal la efectividad de este modelo de incentivos que hay compañías dedicadas a ofrecer servicios de minería o incluso equipos diseñados específicamente para este propósito, usando como referencia de desempeño la cantidad de claves *hash* que pueden probar por segundo **GH/s** (ButterflyLabs 2012).

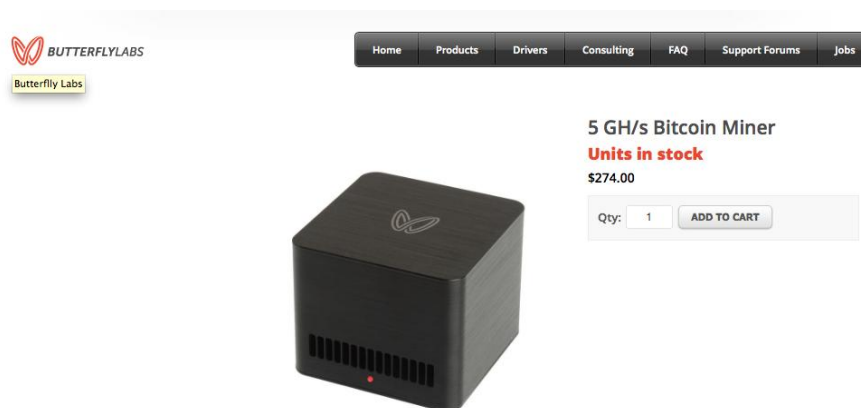


Figura 3.32: Máquina para Minería Butterflylabs.

Fuente: (ButterflyLabs 2012).

3.5 Anonimato

Se discute mucho sobre si el sistema ofrece anonimato o no a los usuarios, debido a que cuestionan su aspecto de carácter público ya que su historial para todas y cada una de las transacciones está al alcance de unos clicks y que la red tenga acceso a toda la información del sistema. (Fergal Reid 2012)

Como ejemplo tomaremos la dirección “**12mmKNqLkXoReZU47Dvnn3KeR4fYkPqjCJ**” y observaremos en la (Figura 3.22) un resumen de la información general que existe sobre esta dirección. Dentro de los valores más relevantes vemos que se menciona el total de **24 transacciones** hasta la fecha relacionada con esta dirección y que posee un monto de **Bitcoins** de **0.00232401** en su saldo final.

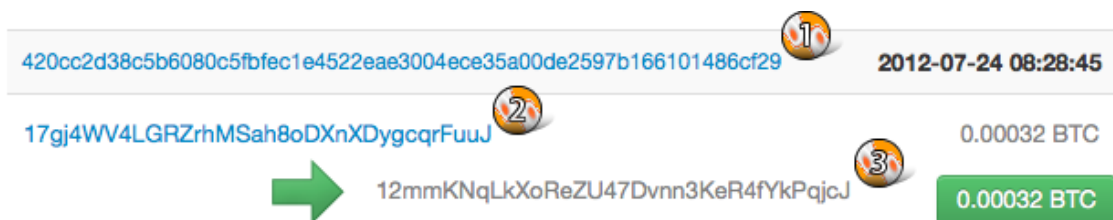


Figura 3.33: Ejemplo de Transacción General.

Fuente: (Blockchain 2013).

En la (Figura 3.27) vemos los elementos de una transacción: fecha y hora del evento 2012-07-24 08:28:45, cantidad de Bitcoins enviados 0.00032 BTC, ID de la transacción (1), dirección Bitcoin del que envía (2), dirección Bitcoin del que recibe (3).

Dirección de Bitcoin

Las direcciones son identificadores que se utilizan para enviar Bitcoins a otra persona.

Resumen	
Dirección	12mmKNqLkXoReZU47Dvnn3KeR4fYkPqjCJ
Hash 160	136ffc03d564a938c392a32ef165ec605687d6f5
Herramientas	Análisis de Marca - Etiquetas Relacionadas - Las salidas no utilizadas



Transacciones	
Número de transacciones	24 
Total recibidas	0.00232401 BTC 
Saldo Final	0.00232401 BTC 



Figura 3.34: Dirección de Bitcoins (General)
Fuente: (Blockchain 2013).

La privacidad se puede apreciar en el modelo: todas las transacciones públicas son anónimas y no hay información personal de las partes involucradas en cierta transacción, contrario a lo que sucede en su homónimo (transacciones bancarias) donde uno debe identificarse con una tercera entidad para realizar el intercambio (Fergal Reid 2012).

A nivel usuario, si éste utiliza la misma clave para todas sus transacciones podría ser rastreado, pero si utiliza una clave distinta para cada transacción se vuelve imposible el relacionarlo (Nakamoto 2008).

Aunque se contara con el tiempo y recursos suficientes para hacer una búsqueda exhaustiva de algún usuario, sólo se podría determinar que dicho usuario en algún momento tuvo control sobre Bitcoins, pero no se podrá determinar ni el monto ni el fin para el que fueron usados (elBitcoin.org 2011).

3.6 Seguridad.

En el artículo “An Analysis of Anonymity in the Bitcoin System” (Fergal Reid 2012) después de una serie de análisis, llegan a la conclusión de que con el monitoreo constante, el equipo adecuado, un rastreo de direcciones IP y la participación de entes dentro del sistema Bitcoin, puede afirmarse que existe una relación entre dos cuentas en específico.

3.6.1 Sistema.

El sistema visto en su totalidad será seguro mientras sean mayoría los nodos honestos, es decir, mientras sea mayor el poder computacional de los nodos confiables en conjunto que el de cualquier grupo de atacantes. Son los participantes

quienes van tomando como válida una transacción usando como prueba el trabajo computacional (Nakamoto 2008).

(Figura 3.21) Muestra un ejemplo de una transacción que NO ha sido aceptada por el sistema, debido a que la cantidad de trabajo no ha sido suficiente para comprobar su veracidad. La transacción “*9114d771194ce9d0e3f88907430969aa29bf4e40020c7a20f08c6b2fb8f3ffd0*” aparece por un tiempo en el historial Bitcoin, con su respectivo mensaje de alerta.

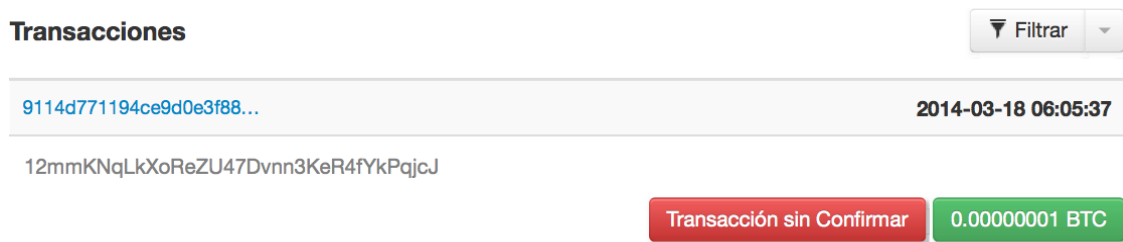


Figura 3.35: Transacción sin Confirmar.

Fuente: (Blockchain 2013).

3.6.2 Transacciones.

Todos los eventos y transacciones que ocurren en el sistema se marcan con una impresión de tiempo ligada a la impresión del evento anterior a esta. Dichas impresiones y los datos del evento son publicados para conocimiento de todos los participantes conectados a la red. (Fergal Reid 2012)

Cada transacción es almacenada en un bloque y se puede observar a detalle la información de dicha transacción como lo muestra la (Figura 3.24) retomando la transacción

“*420cc2d38c5b6080c5bfec1e4522eae3004ece35a00de2597b166101486cf29*” vista anteriormente en la (Figura 3.21) ahora observaremos otros elementos más técnicos de dicha transacción, dentro los que destacan:

Tamaño 225 (bytes): Nos indica el peso en memoria de almacenamiento que ocupa esta transacción.

Hora de Recepción: Momento en que fue enviada al sistema.

Incluidas en el Bloque: Número de bloque en que está almacenada junto con su fecha de integración.

Confirmaciones: Número de Mineros que han confirmado la veracidad de dicha transacción.

Entrada Total: Número de Bitcoins enviados en dicha transacción.

Salida Total: Número total de Bitcoins relacionados a dicha transacción (Incluye los bitcoins enviados por comisiones para la atención de esta transacción).

Comisiones: Monto de Bitcoins otorgados por el emisor como pago para la pronta atención de dicha transacción.

Estimado de BTCs transaccionados: Número de Bitcoins que se estima fueron enviados a una cuenta diferente del emisor.

Transacción Ver información de una transacción de Bitcoin

420cc2d38c5b6080c5fbfec1e4522eae3004ece35a00de2597b166101486cf29

17gj4wW4LGRZrnMSah8oDXnXDygcqrFuuJ



18XdTNUvAbwfcVeWMA68L2DYXJTLkK6LAW
12mmKNqLkXoReZU47Dvnn3KeR4fYkPqjCJ

14.98652 BTC
0.00032 BTC

14.98684 BTC

Resumen	
Tamaño	225 (bytes)
Hora de Recepción	2012-07-24 08:28:45
Incluidas en el Bloque	190505 (2012-07-24 08:39:15 +10 minutos)
Confirmaciones	101801 Confirmaciones
Entradas y Salidas	
Entrada total	14.98734 BTC
Salida Total	14.98684 BTC
Comisiones	0.0005 BTC
Estimado de BTCs transaccionados	0.00032 BTC

Figura 3.36:
Transacción
Detallada.
Fuente:
(Blockchain 2013).

3.6.3 Participantes.

En cuanto a los entes involucrados dentro de la transacción, al ser un sistema **peer-to-peer**, tenemos al que envía Bitcoins y al que los recibe.

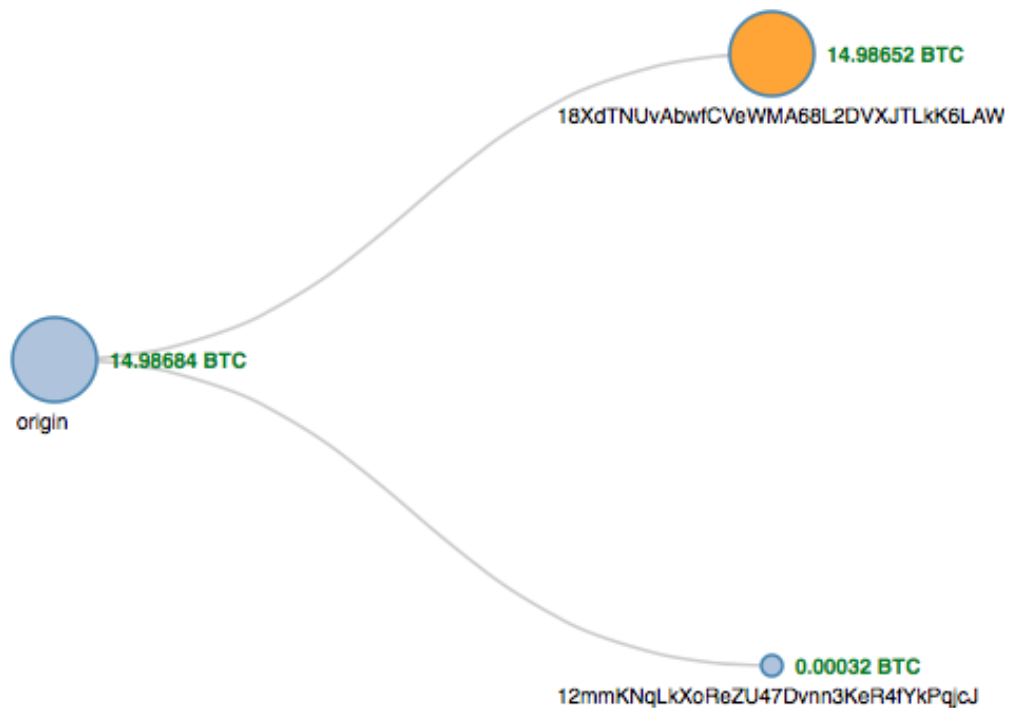


Figura 3.37: Transacciones Peer to Peer.

Fuente: (Blockchain 2013).

A ambos participantes les interesa salvaguardar sus Bitcoins e identificar, ya sea el origen para el que recibe o el destino para el que envía, los Bitcoins. En el caso de la (Figura 3.31) el origen envía 14.98684 Bitcoins a dos destinos cuyas respectivas direcciones y cantidades son las siguientes (Cuadro 3.2):

Cuadro 3.2: Transacción Peer to Peer: Monto de Bitcoins por dirección.

Fuente: (Blockchain 2013).

Dirección	Bitcoins
18XdTNUvAbwfCVeWMA68L2DVXJTLkK6LAW	14.98652
12mmKNqLkXoReZU47Dvnn3KeR4fYkPqjCJ	0.00032

Mantener seguros los Bitcoins depende de cada usuario como lo sería con el dinero en efectivo, con una gran diversidad de circunstancias como dónde tengas guardada la billetera, que uso le des a tu equipo de cómputo, la complejidad de tus claves y otras más (elBitcoin.org 2011).

Por otro lado verificar origen y destino recae en las llaves o claves del sistema mismo, que usan las direcciones. Siendo las públicas conocidas por todos para verificar destinos y las privadas conocidas sólo por el dueño para verificar orígenes (Fergal Reid 2012).

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

An address is a string of letters and numbers, such as 1HULMZEPkEPzCh43BekUJpbLCWfDpN.

Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Private key

Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

The miners' computers are set up to calculate cryptographic hash functions.

Public key

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

Private key

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

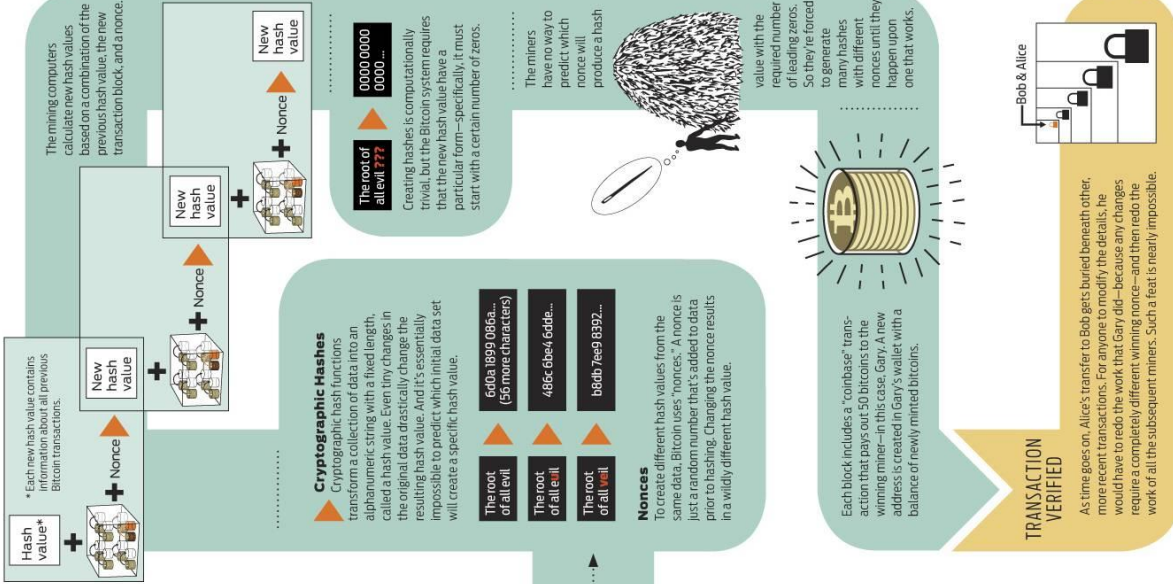


Figura 3.38: Sistema Bitcoin Transacción. Fuente: (trueeconomics. 2013).

CAPÍTULO 4: PERCEPCIONES

4.1 Expertos en Tecnologías de la Información

-**Suren Ter.**- matemático, experto en tecnologías de la información y creador de YouHaveDownloades.com (sitio web que busca llamar la atención sobre la falta de privacidad en Internet) – fue entrevistado recientemente por Andrew, de Privacy Online News. Cuando éste le pregunto qué pensaba acerca de Bitcoin, Suren respondió lo siguiente: “Hay dos aspectos. Desde un punto de vista científico, se trata de un algoritmo muy elegante. Mis felicitaciones a su brillante creador. Socialmente es, también, algo extraordinario: algo así como una versión perfeccionada del oro. Si alguna red social importante o algún fabricante de juegos para redes sociales comenzara a utilizar a Bitcoin como moneda... Wow! Crearía una fuerte demanda; y es difícil predecir las consecuencias, pero generaría un escándalo.”- (Parra 2011).

En este medio tanto los programadores como los especialistas en T.I. y criptografía han aplaudido el ingenioso modelo de seguridad e innovación que este sistema descentralizado ofrece.

Muchos expertos han analizado el código abierto y no han encontrado ninguna vulnerabilidad por la cual preocuparse. Sin embargo critican el que no sea completamente anónimo y que debido al esquema de su funcionalidad, no se vea sostenible a largo plazo (<http://www.slideshare.net/dakami/bitcoin-8776098> 2011).

4.2 Economistas.

El Doctorado en Economía y profesor del Colegio de Economía de la Universidad de Nihon **Tetsuya Saito** en su artículo: “Bitcoin: A Search-Theoretic Approach” incluye en sus conclusiones la viabilidad de la coexistencia del Bitcoin y las monedas actuales (EURO y Dólar), resaltando mucho su inquietud por la postura que debería tomar el Gobierno y su preocupación por mantener el sistema del Bitcoin saludable (Saito 2013).

Algunos economistas no le han prestado mucha atención, como se mencionó antes, debido a que la comparan con elementos conocidos (Agosto 2012).

El hecho es que existen compañías que están generando miles de dólares debido a este nuevo mercado. Empresas como **MtGox** tienen a su disposición casi el 80% de los bitcoins en cuentas de sus usuarios y llevan a cabo cerca de 8 millones de transacciones por día, lo que les genera aproximadamente unos \$276,000 dolares diarios. (Abril 2012).

Monopolios emergentes, como la fusión de **CoinLab** y **Mt. Gox**, provocaron un aumento del 300% en el valor del Bitcoin en menos de 3 meses.

Algunas de las desventajas que los economistas observan son la dificultad de uso, cambio, gasto y/o conversión, aunado al esquema deflacionario sobre el que está montado, pues suponen que si el precio del Bitcoin sigue aumentando la gente no va a querer usarlos (Bonn 2011).

Son pocos economistas los que creen en una moneda no respaldada por un gobierno y los que las apoyan son porque estas combaten radicalmente la inflación.

4.3 Gobierno

El gobierno en general se ve incomodado por la falta de control legal, para actuar en contra de esta nueva tecnología. El lavado de dinero y el abuso del anonimato que ofrece este sistema, para cometer actos ilícitos son algunas de estas consecuencias (FBI 2012).

Es una realidad todo lo mencionado en el estudio hecho por el FBI (FBI 2012). Para comprobarlo basta con navegar un poco en la **Deep WEB** – Páginas o sitios web de difícil acceso, ocultos al usuario y buscadores comunes - y toparse con sitios que ofrecen todo tipo de productos y servicios ilegales a cambio de Bitcoins.

The screenshot shows a website interface for 'USA Citizenship'. At the top left, the text 'USA Citizenship' is displayed in red and white. To the right, there are navigation buttons for 'Products', 'FAQs', 'Register', and 'Login'. The main content area features a heading 'Become a citizen of the USA, real USA passport' and an image of the American flag and the Statue of Liberty. Below the image, there is a block of text describing the offer: 'We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA! It will even work if you arent in the USA yet'. Further text explains the process, mentioning 'Trade secret!', 'We are shipping documents from the USA, international shipping is no problem.', and 'You can use your own name or a new name!'. It also states that 'Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.' At the bottom, there is a table with columns for 'Product', 'Price', and 'Quantity'. The table contains one row: 'Your USA citizenship' with a price of '10000 USD = 17.788 ₿' and a quantity of '1'. A 'Buy now' button is located to the right of the quantity field.

Product	Price	Quantity
Your USA citizenship	10000 USD = 17.788 ₿	1 X Buy now

Figura 4.1: Sitio Deep Web: Venta de Identificaciones Falsas.

Fuente: (Deep Web: Usa Citizenship 2014).

Se pueden encontrar desde identificaciones falsas (Figura 4.1), documentos como pasaportes, ciudadanía, pasando por sitios de apuestas ilegales, venta de drogas (Figura 4.2), lavado de dinero, hasta sitios pornográficos (Figura 4.3), venta de información de compañías o personas, contratación de asesinos a sueldo entre otros.

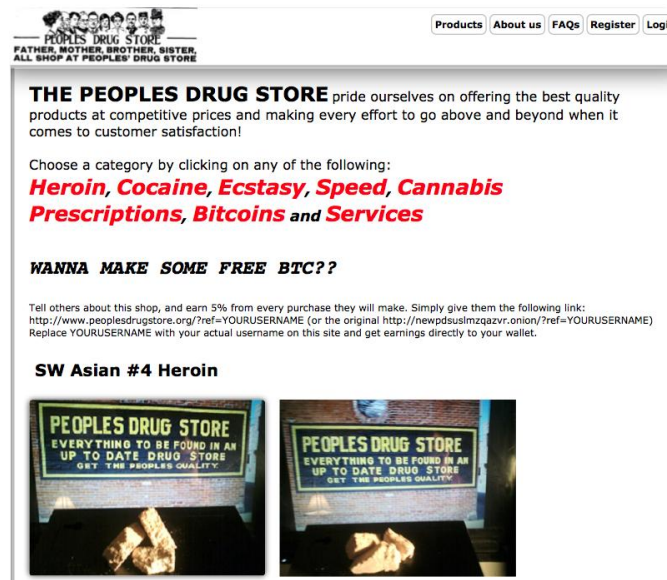


Figura 4.2: Sitio Deep Web: Venta de drogas, prescripciones y otros.

Fuente: (Deep Web: Peoples Drug Store 2014).

En el servicio de lavado de dinero no sólo se ofrece a dinero en cuentas bancarias sino también a lavado de Bitcoins, para aquellas personas que buscan una mayor garantía de anonimato (Figura 4.4).



Figura 4.3: Sitio Deep Web: Lavado de Bitcoins.

Fuente: (Deep Web: Onion Wallet 2014)

Todo esto es la parte negativa del uso que se le da a los Bitcoins, pero también es cierto que todo este ecosistema o mercado ilegal existía antes de la llegada de esta herramienta y era con dinero común o incluso cuentas bancarias con las que se manejaban estos sitios.

Irónicamente el mismo Gobierno reconoce que la gente hace uso y deposita su confianza en los Bitcoins por la misma razón que lo hace en sus Gobiernos: Debido a que pueden intercambiar esta "moneda" por bienes y servicios en la red (Branstad 1993).

4.4 Usuario Final.

Son varios factores los que alejan al usuario común del uso de los Bitcoins y lo vuelven un escéptico de esta nueva herramienta. En sus inicios, lo perciben como algo difícil de utilizar y poco comprensible (BitcoinTalk 2009).

Algunas veces lo comparan con un **esquema Ponzi** – Operación fraudulenta de inversión que implica el pago de intereses con dinero propio de los inversores - y le restan importancia, catalogandolo como un simple sistema de pago por Internet (Ou 2011).

Fácilmente lo ven como algo sin valor ya que no está respaldado por algún Gobierno, lo que, aunado el anonimato de su creador, le resta popularidad dentro del grupo de usuarios comunes.

CAPÍTULO 5: MÉTODOS

5.1 Tasas de Crecimiento.

Se busca demostrar que la tasa de crecimiento del volumen de transacciones de Bitcoins es mayor a la tasa de crecimiento del volumen de Bitcoins en circulación.

$$H_0 : \Delta t = \Delta c$$

$$H_a : \Delta t \neq \Delta c$$

Evaluando los registros de transacciones y de Bitcoins en circulación desde su creación hasta el día de hoy (18/FEB/2014), se obtuvieron los siguientes valores:

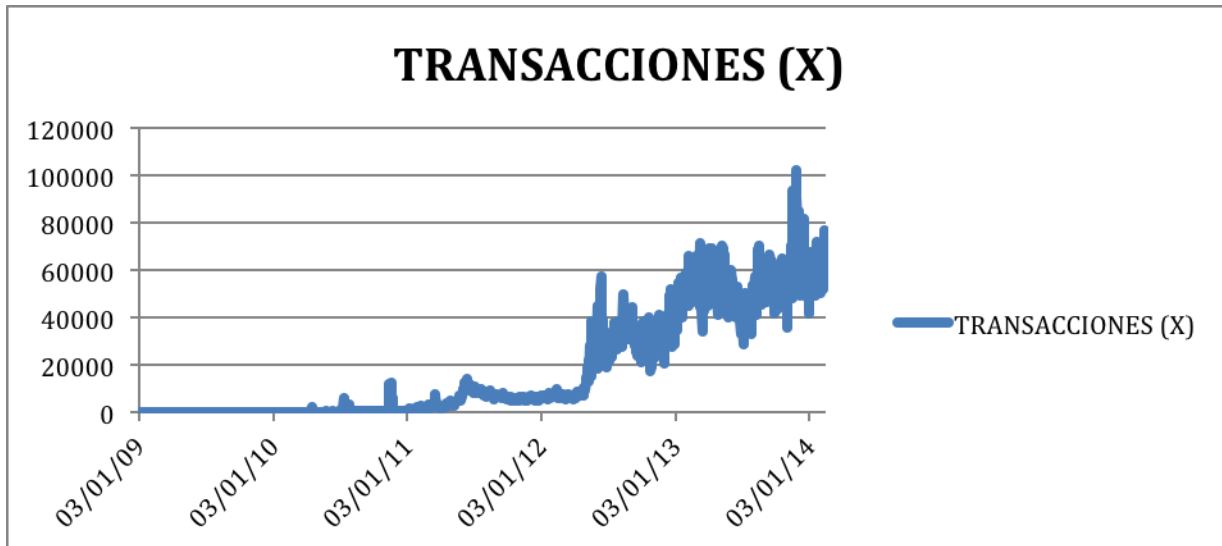


Figura 5.1: Volumen de Transacciones Bitcoin.

Fuente: (Charts 2010)

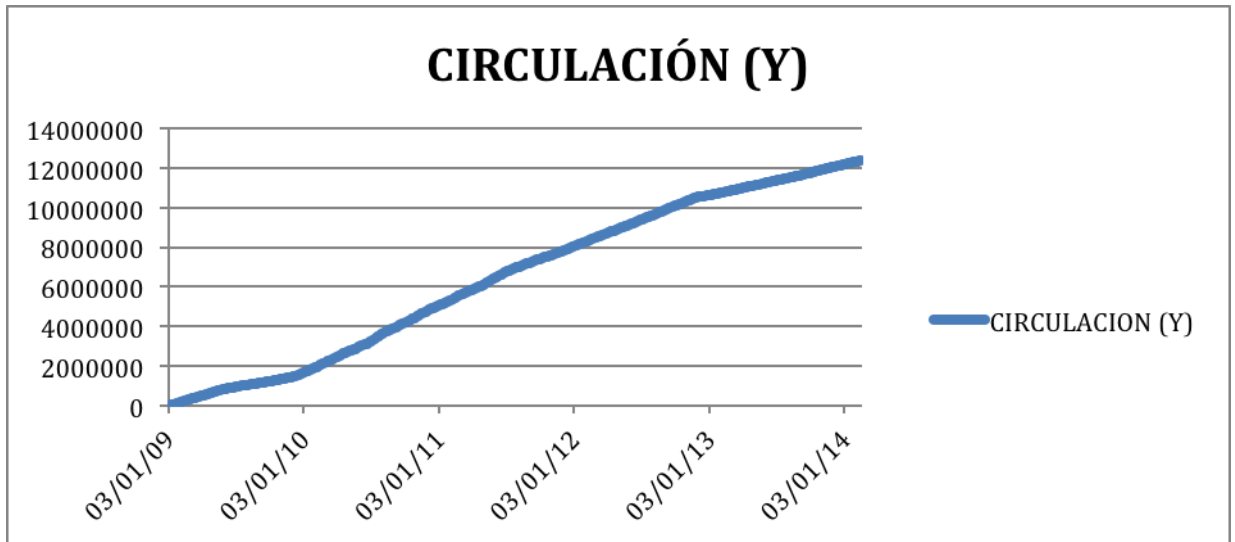


Figura 5.2: Volumen de Bitcoins en Circulación.

Fuente: (Charts 2010)

Cuadro 5.1: Resultados: Tasas de Crecimiento

Tasa de crecimiento del Volumen de Transacciones (x)	Tasa de crecimiento del volumen Bitcoins en circulación (y)
7.82	1.35

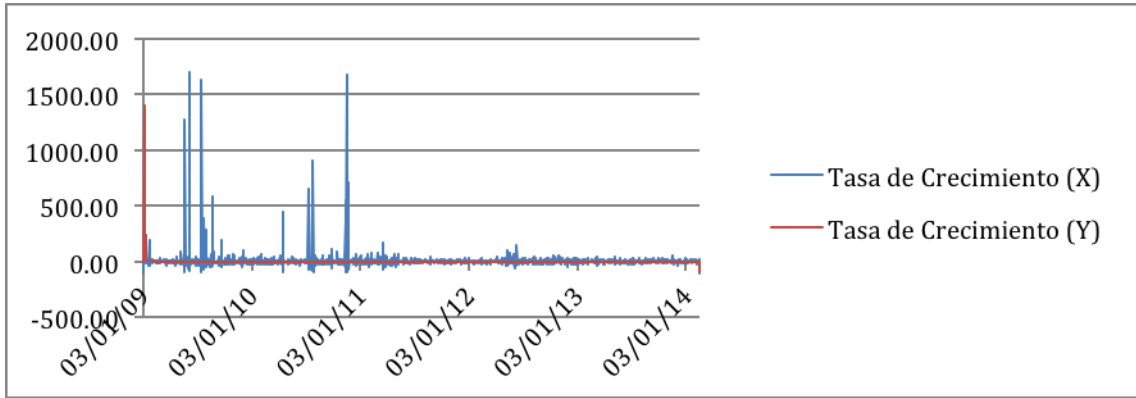


Figura 5.3: Comparación de Tasas de Crecimiento.

5.2 Regresión Lineal.

Con el fin de saber si las variables que se utilizaron en la comparación de tasas de crecimiento se explican una a otra y la relevancia de un modelo usando dichas variables se utiliza la siguiente regresión lineal.

Usando una línea recta con fórmula:

$$\text{Log}(y) = a + b\text{Log}(x)$$

Donde el coeficiente **b** es la pendiente de la recta: el cambio medio que se produce en el número de volumen de circulación de Bitcoins (**y**) por cada unidad de cambio que se produce en volumen de transacciones (**x**). El coeficiente **a** es el punto en que la recta corta el eje vertical: el número de Bitcoins que corresponden a una transacción con volumen de cero.

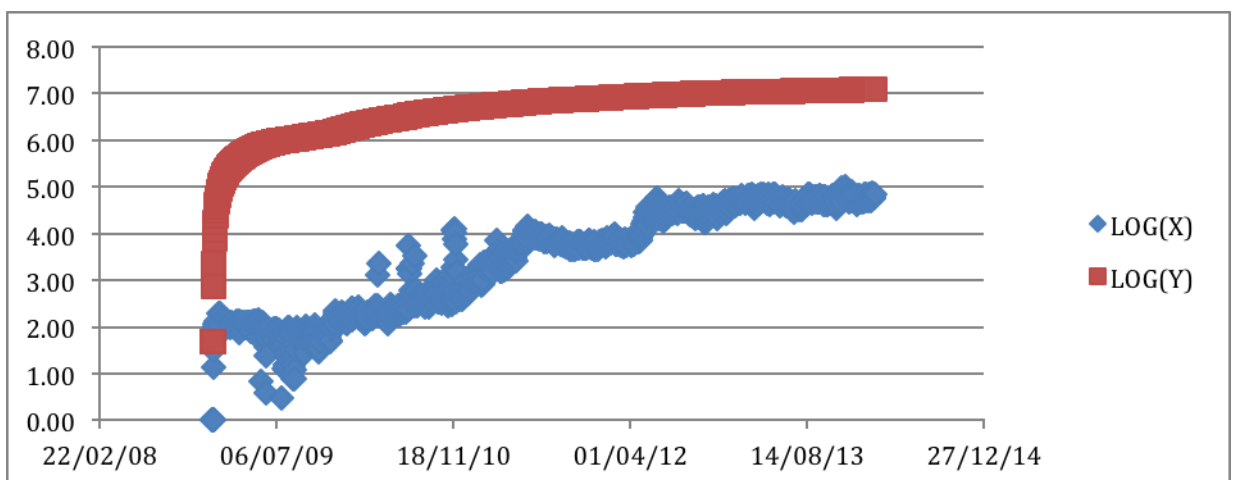


Figura 5.4: Logaritmo de Transacciones y Volumen en Circulación de Bitcoins.

$$\text{LOG}(y) = 5.2245 + 0.4096 * \text{LOG}(x)$$

$$\text{LOG}(\text{Bitcoins en Circulación}) = 5.2245 + 0.4096 * \text{LOG}(\text{Transacciones})$$

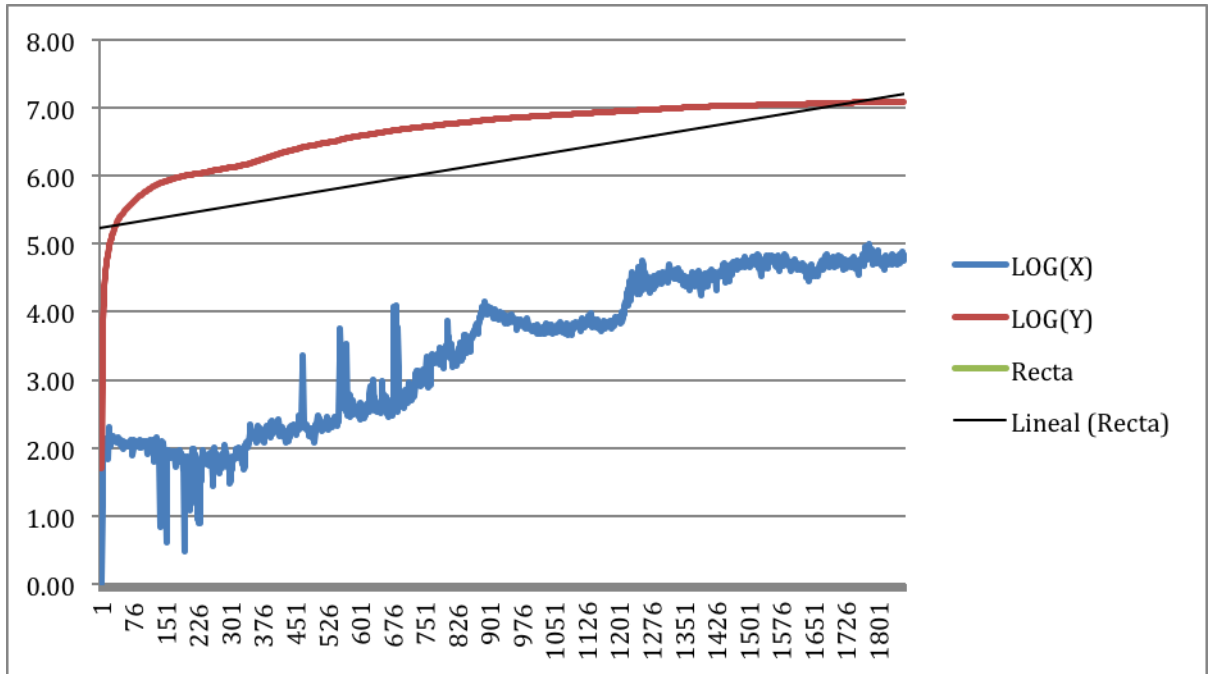


Figura 5.5: Regresión Lineal.

CAPÍTULO 6: RESULTADOS Y DISCUSIÓN

6.1 Resultados del Análisis.

Observando que la tasa de crecimiento del volumen de transacciones es mayor que la del volumen de Bitcoins en circulación la hipótesis $H_0 : \Delta t = \Delta c$ es rechazada.

Existe suficiente evidencia muestral para sustentar que el volumen de transacciones supera al volumen de Bitcoins en circulación.

Cuadro 6.1: Resultados estadísticos de la regresión.

Estadísticos de Regresión	
R	0.80834
R Cuadrado	0.65341
R Cuadrado Ajustado	0.65322
S	0.33136
Número Total de Casos	1865

El coeficiente de correlación lineal simple (**R**) indica que existe un grado de 0.80 de asociación de forma directa entre las variables: el volumen de transacciones y el volumen de Bitcoins en circulación.

Para un $\alpha = 0.05$

$$F = 3,512.17355$$

Debido a que el valor **F** calculado es mayor que al **F0.05** tabular se concluye que existe una relación lineal entre el volumen de transacciones y el volumen de

Bitcoins en circulación y por lo tanto el modelo es apropiado.

CAPÍTULO 7: CONCLUSIONES

7.1 Bitcoin.

Hay que observar el desarrollo del Bitcoin; ya que es una propuesta, una teoría puesta en práctica que ofrece un camino distinto a todo lo antes concebido, seguimos con la interrogante sobre la definición del Bitcoin.

7.1..1 Ventajas.

El sistema Bitcoin ofrece una solución al doble gasto bastante elegante y muy superior a las monedas electrónicas actuales, como se puede apreciar en (Nakamoto 2008).

Aunque queda claro que no existe el anonimato total, es bastante robusta la manera en que protege la información de consumo de sus usuarios. El anonimato no es un objetivo del sistema Bitcoin y es evidente que hay que tomar medidas complementarias si se quiere mantener una privacidad mayor a la ofrecida por el sistema mismo.

El sistema descentralizado ayuda a preservar y proteger la integridad de la información que este almacena, ya que se vuelve bastante costoso el corromperlo.

En la (Figura 7.1) se muestra en verde a países que ya lo han adoptado (Beigel 2013) en rojo los que están tratando de erradicarlo y en amarillo los que buscan regularlo (Hill 2013) (FBI 2012). Lo que es cierto es que las tiendas de comercio electrónico y el sector turístico se han visto impulsados por este instrumento. Desde una pizza (bitcointalk 2010), pasando por un automóvil último modelo (Lavrinc 2013), hasta fertilización in-vitro (Goldhill 2013) e incluso viajes espaciales (El Economista 2014), han sido adquiridos con Bitcoins.

7.2 Análisis

Se determinó el comportamiento del Bitcoin, su funcionamiento general y su origen. En cuanto a la aceptación y el uso de la moneda, gracias al volumen de transacciones realizadas hasta la fecha, se logró encontrar una relación lineal demostrando la importancia y relación que existe entre el volumen de transacciones y el volumen de Bitcoins en circulación.

Pudimos observar que la tendencia tanto del volumen en circulación y el volumen de transacciones va en aumento, y que es radicalmente superior el aumento del volumen de transacciones al aumento del volumen de Bitcoins en circulación.

Son muchos los paradigmas que hay que romper y ambientes económicos de ciertos países que habría que estabilizar, para que el dinero electrónico pase a ser una única divisa que una a todo el mundo como una sola nación. Lo que el Bitcoin nos está demostrando, es que es posible usar una divisa electrónica a la par de las divisas convencionales, y que existe una demanda y un mercado para este tipo de instrumentos.

Hay que enfatizar que el uso del Bitcoin no es para preservar valor; más bien, es un medio de intercambio muy volátil y que la importancia del Bitcoin no radica en el valor de la criptomoneda sino en el sistema mismo.

BIBLIOGRAFÍA

- Charts, Bitcoin. 2010. Bitcoin Charts. <http://bitcoincharts.com/> (Consultado: 30 de Agosto de 2014).
- Casascius. 2011. Physical Bitcoins by Casascius. <https://www.casascius.com/> (Consultado: 12 de Marzo de 2012).
- Lavrinc, Damon. 2013. Someone Bought a Tesla Model S With Bitcoins. <http://www.wired.com/autopia/2013/12/tesla-bitcoin/> (Consultado: 13 de Febrero de 2014).
- Localbitcoins. 2012. <https://localbitcoins.com/iframe/#> (Consultado: 31 de Abril de 2013).
- Loom. 2012. https://loom.cc/help#what_is_loom (Consultado: 23 de Octubre de 2013).
- AlAhmad Mohammad, Fakhri Alshaikhli Imad. 2013. Broad View of Cryptographic Hash Functions. International Journal of Computer Science Issues, Julio de 2013: 1.
- Andersen, Gavin. Faucet. Gavin Andersen. 2010. <http://testnet.freebitcoins.appspot.com/> (Consultado: 8 de Febrero de 2012).
- Apple. 2014. <https://developer.apple.com/xcode/> (Consultado: 4 de Mayo de 2014).
- Black, Adam. 2002. Hashcash - A Denial of Service Counter-Measure. 12. Vol. Abril. 2013.
- Blockchain. 2013. <https://blockchain.info/es/charts> (Consultado: 18 de Febrero de 2014).
- Beigel, Ofir. 2013. BITCOIN WORLDWIDE LEGAL AND ADOPTION STATUS. <http://99bitcoins.com/bitcoin-worldwide-adoption-status/> (Consultado: 9 de Abril de 2014).
- Bitcoin Block Explorer.

- Home - Bitcoin Block Explorer. 2013. <http://blockexplorer.com/> (Consultado: 2013).
- Bitcoin.it. 2013. <https://en.bitcoin.it/wiki/History> (Consultado: 24 de Septiembre de 2013).
- Bitcoin.org. 2009. <https://bitcoin.org/> (accessed 19 de Marzo de 2014).
- BitcoinTalk. 2009. Bitcoin Forum. <https://bitcointalk.org/> (Consultado: 24 de Septiembre de 2012).
- Bitcointalk. 2010. <https://bitcointalk.org/index.php?topic=137.0> (accessed 12 de Enero de 2012).
- Bitbills Inc. 2011. Bitbills. <http://www.bitbills.com/> (Consultado: 12 de Agosto de 2012).
- Bonn. 2011. The Bursting of Bitcoin Bubble. The Economist, 21 de Octubre de 2011.
- Branstad, Dennis K. Report of the Nist Workshop on Digital Signature Certificate anagement. 1993. DIANE Publishing.
- ButterflyLabs. ButterflyLabs. 2012. <https://products.butterflylabs.com/5-gh-s-bitcoin-miner.html> (Consultado: 24 de Septiembre de 2013).
- Deep Web. 2014. Onion Wallet. <http://ow24et3tetp6tvmk.onion/> (Consultado: 22 de Marzo de 2014).
- Deep Web. 2014. Pedo City. <http://pedocity3bxrocbj.onion/login/> (Consultado: 22 de Marzo de 2014).
- Deep Web. 2014. Peoples Drug Store - The Darkweb's Best Online Drug Supplier!... . 22 de Marzo de 2014. <http://newpdsuslmzqazvr.onion/> (Consultado: 22 de Marzo de 2014).
- Deep Web. 2014. USA Citizenship - Become a citizen of the USA today, possible ... 22 de Marzo de 2014. <http://xfnwyig7olypdq5r.onion/> (accessed 22 de Marzo de 2014).
- DomainTools. 2008. Whois. <http://whois.domaintools.com/bitcoin.org> (Consultado: 24 de Septiembre de 2013).

- El Economista. 2014. Winklevoss pagarán con bitcoins viaje al espacio. <http://eleconomista.com.mx/entretenimiento/2014/03/05/winklevoss-pagaran-bitcoins-viaje-espacio> (Consultado: 12 de Marzo de 2014).
- ElBitcoin.org. 2011. La moneda del Futuro -Qué es, cómo funciona y porqué cambiará el mundo. (Consultado: 15 de Julio de 2011).
- FBI. 2012. (U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. FBI. <http://cryptome.org/2012/05/fbi-bitcoin.pdf> (Consultado: 2 de Mayo de 2012).
- Fergal Reid, Martin Harrigan. 2012. An Analysis of Anonymity in the Bitcoin System. Cornell University Library. <http://arxiv.org/pdf/1107.4524.pdf> (Consultado: 30 de Agosto de 2013).
- Forbes. Forbes. 2012. <http://www.forbes.com> (accessed 24 de Septiembre de 2012).
- Foundation, P2P. 2011. <http://p2pfoundation.net/Loom> (Consultado: 30 de Agosto de 2013).
- Ghassan O. Karame, Elli Androulaki, Srdjan Capkun. 2012. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin.
- Goldhill, Olivia. 2013. First 'Bitcoin baby' is a girl, born last year. <http://www.telegraph.co.uk/technology/internet/10112717/First-Bitcoin-baby-is-a-girl-born-last-year.html> (Consultado: 13 de Febrero de 2014).
- Grinberg, Reuben. 2011. Bitcoin: An Innovative Alternative Digital Currency . Texas, Austin.
- Hill, Kashmir. 2013. Bitcoin in China: The Fall-out From Chinese Government Banning Real World Use. <http://www.forbes.com/sites/kashmirhill/2013/12/06/bitcoin-in-china-the-fall-out-from-chinese-government-banning-real-world-use/> (Consultado: 4 de Enero de 2014).

- Adam Black. 2002. A Denial of Service Counter-Measure. Hashcash. <http://www.hashcash.org/papers/hashcash.pdf> <http://www.hashcash.org/> (Consultado: 13 de Febrero de 2013).
- Dan Kaminsky. 2011. Some Thoughts on Bitcoin. <http://www.slideshare.net/dakami/bitcoin-8776098>. (Consultado: 23 de Agosto de 2011).
- Kolivas. CGMiner. 2011. <https://github.com/ckolivas/cgminer> (Consultado: 19 de Marzo de 2004).
- Kolivas, Con. CGminer. 2011. <https://github.com/ckolivas/cgminer> (Consultado: 4 de Mayo de 2014).
- Krugman, Paul. 2013. Bitcoin Is Evil. The New York Times, 28 de Diciembre de 2013.
- —. Golden Cyberfettters. 2011. The New York Times, 7 de Septiembre de 2011.
- Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org.
- Olesen, Lasse Birk. 2012. BitcoinNordic. https://bitcoinnordic.com/index_da.html (Consultado: 1 de Abril de 2014).
- O'Mara, John. 2013. MacMiner. <http://fabulouspanda.co.uk/macminer/27> de Diciembre de 2013. (accessed 18 de Marzo de 2014).
- Ou, George. 2011. Hightechforum. <http://www.hightechforum.org/bitcoins-a-crypto-geek-ponzi-scheme/> 10 de Enero de 2011. (Consultado: 2012 de Septiembre de 2012).
- Parra, Sergio. 2011. La Bitcoin: la moneda digital que ya superará. <http://www.xatakaciencia.com/tecnologia/la-bitcoin-la-moneda-digital-que-ya-supera-el-dolar>. 20 de Junio de 2011. (Consultado: 14 de Enero de 2012).
- Saito, Tetsuya. 2013. Bitcoin: A Search-Theoretic Approach. Tokyo, Nihon, Mayo de 2013.
- Simonite, T. 2011. ¿Qué es Bitcoin, y por qué es importante? MIT Technology Review.

http://www.technologyreview.es/read_article.aspx?id=37638 25 de Mayo de 2011. (Consultado: 12 de Febrero de 2012).

- The Hindu. 2013. Thehindu. <http://www.thehindu.com/business/Industry/bitcoin-gains-currency-in-india/article5422252.ece> 4 de Diciembre de 2013. (Consultado: 4 de Diciembre de 2013).
- Tilborg, Henk C.A. van. 2005. Encyclopedia of Cryptography and Security. Springer Science+Business Media, Inc.
- Tiwari Harshvardhan, Asawa Krishna. 2010. Cryptographic Hash Function: An Elevated View. European Journal of Scientific Research, Julio de 2010: 452.
- International Journal of Computer Science and Information Security, Febrero de 2010.
- Trueeconomics. 2013. A Secure Hash Function MD-192 With Modified Message Expansion. Trueeconomics. <http://trueeconomics.blogspot.mx/2013/05/1252013-how-bitcoin-works.html> 12 de Mayo de 2013. (Consultado: 20 de Agosto de 2013).
- Weusecoins. Your Portal into the world of Bitcoin. 2011. <https://www.weusecoins.com/getting-started.php> (Consultado: 3 de Febrero de 2012).
- Wikipedia. 2014. Legality of Bitcoins by country. http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country (Consultado: 9 de Abril de 2014).
- Wikipedia. 2013. Myths. <https://en.bitcoin.it/wiki/Myths> (Consultado: 14 de Agosto de 2013).
- Wikipedia. 2012. http://en.wikipedia.org/wiki/History_of_Bitcoin (Consultado: 23 de Noviembre de 2013).

GLOSARIO

Algoritmo

Conjunto de: pasos, actividades, instrucciones o cálculos; para resolver un problema abstracto.

Algoritmos criptográficos

Algoritmo que modifica los datos de un documento con el objetivo de alcanzar algunas características de seguridad como autenticación, seguridad y confidencialidad.

Amazon Coins

Medio digital que permite a los usuarios de Amazon adquirir aplicaciones y juegos dentro de amazon.com

Cadena de bloques

Listado seriado por fecha de aparición de todos los bloques existentes de transacciones.

Bitcoin

La primera moneda digital descentralizada, basada en una red punto a punto.

Bloque

Determinado volumen de transacciones agrupadas, con clave única, para su fácil registro y seguimiento.

cartera digital

Archivo que contiene la información de identidad y montos del dinero electrónico, parecido a una cuenta bancaria o una tarjeta de crédito.

criptomoneda

Moneda electrónica que utiliza protocolos, algoritmos o sistemas de encriptación.

Deep Web

Todo el conjunto de contenido y sitios web no accesibles por los motores de búsqueda convencionales o que presentan una serie de requisitos como serían contraseñas, direcciones IP específicas u otros, para su acceso.

Genesis Block

Primer bloque generado, que dio inicio al sistema Bitcoins.

Facebook Credits

Moneda virtual que permite a los usuarios de Facebook comprar artículos o créditos dentro de las aplicaciones diseñadas para esta plataforma.

Linden Dollars

Moneda virtual de la economía dentro del video juego "Second Life".

Loom

Es un sistema de pagos anónimo y centralizado de registro de cuentas para monedas electrónicas. (Foundation 2011) (Loom 2012)

minería

Acción que realizan los mineros para obtener Bitcoins. Atender volúmenes de transacciones y validar bloques.

mineros

Actores activos dentro del sistema descentralizado Bitcoin, que atienden peticiones de transacciones y validan bloques mediante el uso de sistemas computacionales.

MtGox

Sitio mas grande de trading de Bitcoins.

Open-Source

Es la expresión con la que se conoce al software distribuido y desarrollado libremente. También llamado Código abierto.

Pay-Pal

Una compañía de comercio electrónico enfocada en facilitar pagos y envío de dinero por internet.

Peer-to-Peer

Se refiere a la estructura de una red, en forma de pares, punto a punto o entre iguales. Donde no siempre se tienen servidores y clientes fijos, sino que en ocasiones clientes actúan de servidores y viceversa.

Slashdot

Sitio de noticias de ciencia y tecnología de la compañía estadounidense Dice Holdings Inc.

Transacción

Suceso efectuado entre pares participantes de la red. Proceso de envío y recepción de Bitcoins.

World of Warcraft Gold

Oro digital dentro del mundo del video juego “world of warcraft” con el que los usuarios comercian